Review: Active Directory Auditing Tools p. 53

Windows® IT Pro

A PENTON PUBLICATION

SEPTEMBER 2011 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU

Explore Office 365 p. 21

Power, performance and trusted experience. Precisely what you need.

The IBM System x3650 M3 Express® server with the latest Intel® Xeon® processor 5600 series can help increase productivity and minimize costs. Featuring a 55% increase in processing power,[1] you'll be able to drive business results faster and can achieve a return on your investment in up to three months.[2] Furthermore, with the valuable expertise of IBM Business Partners, you can create an IT environment optimized to keep pace with your growing business.

Rated No. 1 in Server Customer Satisfaction by TBR for the 6th consecutive quarter.[3]

IBM System x3650 M3 Express

$2,799

OR $72/MONTH FOR 36 MONTHS[4]

PN: 7945-E6U

- Outstanding performance for most business applications
- Unprecedented low price point
- Readily available inventory—stocked in the channel

IBM System x3400 M3 Express

$1,699

OR $44/MONTH FOR 36 MONTHS[4]

PN: 7379-E5U

- Ideal tower server for small/midsized and distributed businesses
- Optimum performance and processing capability at a low cost
- Readily available inventory—stocked in the channel

IBM System Storage® DS3500 Express

$5,499

OR $141/MONTH FOR 36 MONTHS[4]

PN: 1746-A2S

- External SAS switch support
- 10 GB iSCSI
- Expands to 192 drives per system

Get the whitepaper

See how IBM consistently meets high customer expectations.

ibm.com/systems/satisfaction

Contact the IBM Concierge to help you connect to the right IBM Business Partner.

1 866-872-3902 (mention 601BB27W)

Or Search x3650m3

intel Xeon inside™

Powerful. Intelligent.

[1]x3650 M3: 931,658 SPECjbb2005 bops 155,276 bops/JVM; Intel Xeon X5690 2 chips/12 cores. x3650 M2: 598,924 SPECjbb2005 bops 149,731 bops/JVM; Intel Xeon X5570 2 chips/8 cores. Results as of 4/5/11. http://www.spec.org/jbb2005/results. SPEC and SPECjbb are registered trademarks of Standard Performance Evaluation Corporation (SPEC). [2]Based on comparing previous generation, 200 servers IBM eServer xSeries 346 (3.0GHz) (2Ch/2Co) to new generation 10 servers IBM x3550 M3 (Xeon E5650) 2.66GHz (2x6) using the IBM Consolidation Evaluation tool. [3]TBR 4Q10 x86-Based Servers: Corporate IT Buying Behavior and Customer Satisfaction Study, February 2011. [4]Global Financing offerings are provided through IBM Credit LLC in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government customers. Monthly payments provided are for planning purposes only and may vary based on your credit and other factors. Lease offer provided is based on an FMV lease of 36 monthly payments. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice. IBM hardware products are manufactured from new parts or new and serviceable used parts. Regardless, our warranty terms apply. For a copy of applicable product warranties, visit http://www.ibm.com/servers/support/machine_warranties. IBM makes no representation or warranty regarding third-party products or services. IBM, the IBM logo, System Storage and System x are registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. For a current list of IBM trademarks, see www.ibm.com/legal/copytrade.shtml. Intel, the Intel logo, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries. All other products may be trademarks or registered trademarks of their respective companies. All prices and savings estimates are subject to change without notice, may vary according to configuration, are based upon IBM's estimated retail selling prices as of 04/29/11 and may not include storage, hard drive, operating system or other features. Reseller prices and savings to end users may vary. Products are subject to availability. This document was developed for offerings in the United States. IBM may not offer the products, features, or services discussed in this document in other countries. Contact your IBM representative or IBM Business Partner for the most current pricing in your geographic area.

C O N T E N T S

COVER STORY

FEATURES

INTERACT

IN EVERY ISSUE

Access articles online at www.windowsitpro.com. Enter the article ID (located at the end of each article) in the InstantDoc ID text box on the home page.

Windows IT Pro

A PENTON PUBLICATION

SEPTEMBER 2011

VOLUME_17 NO_9

COLUMNS

CONTENTS

PRODUCTS

Windows IT Pro

EDITORIAL

Editor in Chief
Amy Eisenberg amy@windowsitpro.com

Senior Technical Director
Michael Otey motey@windowsitpro.com

Technical Director
Sean Deuby sean@windowsitpro.com

Senior Technical Analyst
Paul Thurrott paul@windowsitpro.com

Industry News Analyst
Jeff James jjames@windowsitpro.com

Custom Group Editorial Director
Dave Bernard dbernard@windowsitpro.com

Developer Content
Anne Grubb agrubb@windowsitpro.com

Exchange & Outlook
Brian Winstead bwinstead@windowsitpro.com

Systems Management, Networking, Hardware
Jason Bovberg jbovberg@windowsitpro.com

Security, Virtualization
Jeff James jjames@windowsitpro.com

SharePoint
Caroline Marwitz cmarwitz@windowsitpro.com

SQL Server
Megan Keller mkeller@windowsitpro.com

Editorial Web Architect
Brian Reinholz breinholz@windowsitpro.com

CONTRIBUTORS

SharePoint and Office Community Editor
Dan Holme danh@intelliem.com

Senior Contributing Editors
David Chernicoff david@windowsitpro.com
Mark Minasi mark@minasi.com
Paul Robichaux paul@robichaux.net
Mark Russinovich mark@sysinternals.com
John Savill john@savilltech.com

Contributing Editors
Alex K. Angelopoulos aka@mvps.org
Michael Dragone mike@mikerochip.com
Jeff Fellinge jeff@blackstatic.com
Brett Hill brett@iisanswers.com
Darren Mar-Elia dmarelia@windowsitpro.com
Tony Redmond 12knocksinna@gmail.com
Eric B. Rux ericbrux@whshelp.com
William Sheldon bsheldon@interknowlogy.com
Curt Spanburgh cspanburgh@scg.net
Orin Thomas orin@windowsitpro.com
Douglas Toombs help@toombs.us
Ethan Wilansky ewilansky@windowsitpro.com

ART & PRODUCTION

Production Director
Linda Kirchgesler linda@windowsitpro.com

Senior Graphic Designer
Matt Wiebe matt.wiebe@penton.com

ADVERTISING SALES

Publisher
Peg Miller pmiller@windowsitpro.com

EMEA Managing Director
Irene Clapham irene.clapham@penton.com

Director of IT Strategy and Partner Alliances
Birdie J. Ghiglione birdie.ghiglione@penton.com
619-442-4064

Online Sales Development Director
Amanda Phillips amanda.phillips@penton.com

Key Account Director
Chrissy Ferraro christina.ferraro@penton.com
970-203-2883

Account Executives
Barbara Ritter barbara.ritter@penton.com
858-367-8058
Cass Schulz cassandra.schulz@penton.com
858-357-7649

Client Project Managers
Michelle Andrews 970-613-4964
Kim Eck 970-203-2953

Ad Production Supervisor
Glenda Vaught glenda.vaught@penton.com

MARKETING & CIRCULATION

Customer Service service@windowsitpro.com

IT Group Audience Development Director
Marie Evans marie.evans@penton.com

Marketing Director
Sandy Lang sandy.lang@penton.com

CORPORATE

PENTON

Chief Executive Officer
Sharon Rowlands sharon.rowlands@penton.com

Chief Financial Officer/Executive Vice President
Nicola Allais nicola.allais@penton.com

TECHNOLOGY GROUP

Senior Vice President, Technology Media Group
Kim Paulsen kpaulsen@windowsitpro.com

WRITING FOR *WINDOWS IT PRO*
Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

LIST RENTALS
Contact MeritDirect, 333 Westchester Avenue, White Plains, NY or www.meritdirect.com/penton.

REPRINTS
Diane Madzelonka, Diane.madzelonka@penton.com, 216-931-9268, 888-858-8851

One Small Spark Can Destroy Your Entire Forest.

Be Prepared for an Active Directory Disaster.

A small glitch in Active Directory could turn into disaster for your business. Are you ready if the worst should happen? Learn how proper planning and the right tools can help you quickly recover – or prevent altogether – Active Directory catastrophes. Download "That Dreaded Day: Active Directory Disasters and Solutions for Preventing Them."

Read the white paper at *www.quest.com/ADDisasterPrevention*

Get the free mobile app at
http://gettag.mobi

QUEST SOFTWARE®
Simplicity At Work™

Otey

"Putting vital corporate assets into a publicly accessible location such as the cloud is definitely a concern for IT pros."

The First Steps to the Cloud

Office 365 and private cloud are less risky technologies for IT pros to consider

This past spring I participated in several events with Microsoft and EMC where we met with IT professionals from many different types of businesses. We discussed a number of topics revolving around the evolution of the data center, including virtualization and the advent of cloud computing. Virtualization is clearly a mainstream technology that almost everyone is using. However, in spite of the deluge of cloud computing marketing messages from all the cloud vendors, most of the IT professionals in attendance viewed the cloud as a future technology that's still on the horizon. In spite of what the vendors of various cloud offerings might want you to think, these IT pros were not clamoring for cloud solutions.

Don't get me wrong. There was a lot of interest in the cloud and in the different types of cloud solutions that are available. However, for the most part, the cloud is still clearly an exploratory technology, not one that IT pros are ready to jump into with both feet. Attendees expressed an interest in learning about how to take better advantage of virtualization both in regard to server consolidation as well as how to move into application virtualization. For the cloud, the interest was mostly about trying to define what the cloud is and then to gauge the benefits that are offered by the different types of cloud solutions.

I see a number of factors that make real customers reticent about cloud computing. First, this reluctance, no doubt, is in part due to the fact that most companies have already made very significant investments in their on-premises infrastructure. Sure, there will always be new start-ups and perhaps for them the cloud might hold greater appeal. But the fact is that by and large today's corporate IT infrastructure is already established—and it works. Today's cloud offerings aren't providing these businesses with any essential functionality that they don't already have. Moving incrementally to the cloud is a possibility, but that approach involves the unknown and risk, both of which are factors IT pros like to avoid.

Next, in spite of all the hype, every single major cloud vendor has had high profile outages in the last year. Everyone has heard of these outages and although cloud proponents quickly downplay these failures, most IT professionals believe the public cloud is an immature technology and anything that's based on the Internet is going to experience downtime.

Finally, there are the questions of performance and security. Even if the public cloud is up, it's a shared solution and it might not perform as well as dedicated servers. Putting vital corporate assets into a publicly accessible location such as the cloud is definitely a concern for IT pros I talked to.

However, although IT pros shared concerns about the public cloud, two scenarios in particular were seen as viable options: Office 365 and other immediately usable Software as a Service (SaaS) solutions, and the private cloud. Office 365 and other SaaS solutions hold appeal because they are ready-to-use solutions. In the case of Office 365, the application isn't seen as mission critical. In other words, it's OK if it doesn't work part of the time. Cloud availability issues aren't a showstopper. Next, businesses know they are struggling with ways to keep desktop Office installations updated. Many are using older versions of Office, and upgrading to each subsequent newer version involves a lot of cost and effort. Finally, the concept of using these types of services for applications really isn't anything new. Many businesses already use web-based software applications such as SalesForce.com.

Unlike the public cloud, which is an entity shrouded in mystery and not just a little bit of confusion, the private cloud was perceived to be a much more appealing and approachable possibility with the IT pros I talked to. Because the private cloud is built on top of your own infrastructure using technologies such as virtualization that are already in widespread use, there's a much higher degree of confidence in the private cloud. Concerns about public access, Internet outages, and security also go away. The private cloud is comprised of collections of virtual machines. Pools of similarly configured virtual machines can be managed as a single service. Technologies such as Hyper-V Live Migration or VMware VMotion are used for dynamic workload balancing and power management. The private cloud is the next step in the evolution of the data center and products such as VMware's vCloud Director and Microsoft's upcoming Virtual Machine Manager 2012 enable you to create and manage a private cloud that's built on top of your existing IT infrastructure.

SaaS and private cloud options require less risk from the IT pro and are likely to be adopted before we see major migrations to the public cloud.

InstantDoc ID 139968

MICHAEL OTEY (motey@windowsitpro.com) is senior technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).

James

"The consumerization of IT is continuing to have an impact on enterprise platform and software adoption, and we're likely to see more social media features finding their way into our business applications."

Facebook for the Enterprise: Potential or Pipedream?

Vendors offer products and services that bring social media into the workplace

With more than 750 million users, Facebook has emerged as the dominant social media platform. People are using Facebook to share photos, chat with friends, and keep in touch with family members and colleagues across the globe. Despite some legitimate privacy and security concerns, Facebook has paved the way for other social media offerings such as Twitter, FourSquare, Quora, GoWalla, and Google+.

Over the past few years, several companies have been working on platforms to bring aspects of social media and social networking into the enterprise. According to a July 2011 social business survey conducted by IDC, 41 percent of survey respondents indicated that they had some sort of social business initiative underway. The IDC report cautioned that the scope, objectives, and maturity of these initiatives varied widely, but the report also stressed that social business software adoption and interest is increasing (bit.ly/nHCFLw).

Salesforce.com CEO Mark Benioff—in a guest post last year on the website TechCrunch (http://techcrunch.com/2010/02/24/the-facebook-imperative/)—urged the enterprise software industry to look to Facebook as a model for how to re-imagine collaboration and communication in the enterprise. "We need to transform the business conversation the same way Facebook has changed the consumer conversation. Market shifts happen in real time, deals are won and lost in real time, and data changes in real time," Benioff wrote. "Yet the software we use to run our enterprises is in anything but real time. We need tools that work smarter, make better use of new technology (like the mobile devices in everyone's hands), and fully leverage the opportunities of the Internet."

A number of companies are trying to do exactly that. Microsoft's ubiquitous SharePoint reigns as the current king of document and content sharing, but is admittedly weak on social media functionality. Services such as Yammer and Salesforce Chatter offer some of the functionality of Facebook for internal use; Salesforce Chatter brings Facebook-like social networking functionality to the core Salesforce.com customer relationship management (CRM) Software as a Service (SaaS) platform. Some IT departments have preferred those services for their ease of deployment (both are SaaS offerings) and similarity to existing social media platforms. Convofy is another player in the field, and is trying to find itself a niche in the burgeoning social enterprise space by focusing on integration between existing platforms.

Jive Software has taken a blank-slate approach, focusing more on people engagement than document management. "We think the best strategy is to design the platform around engaging people, not documents," said Tim Zonca, Jive's director of product marketing. "We wanted to be social from the ground up."

Newsgator's Social Sites builds on top of SharePoint and adds more social media elements, a strategy that capitalizes on Microsoft's vast SharePoint installed base. Brad Feld, managing director of the Foundry Group (a venture capital firm that invests in Newsgator), believes that building social media functionality on top of SharePoint is an attractive solution. "Microsoft SharePoint provided an incredible platform for this, both as a technology backbone as well as the broad adoption it has seen throughout large enterprises," Feld says.

Newsgator CEO J.B. Holston elaborated on his company's Microsoft-centric strategy with Social Sites. "We focused on the Microsoft stack, with SharePoint as the focus but now including all the Office 365 components (Exchange, Office, and Lync, too) because of their ubiquity," Holston said. "Since we leverage the Microsoft stack fundamentally, our offerings have fundamental search, single profile, security, scalability, and globalization/localization benefits that are magnitudes ahead of the competition. SharePoint alone has over 100 million paid seats worldwide, is Microsoft's fastest growing server product ever, and has been adding 20,000 seats per day every day for the last five years."

Other vendors are angling for a piece of the social business market, including IBM with their IBM Connections platform. "We offer three different deployment options: on-premise, hosted (through IBM or IBM partners), and multi-tenant with IBM Lotus Live," said senior marketing manager for IBM Connections Christopher Lamb. "We also leverage IBM's expertise with BI to combine social data with analytics. We're using social analytics and filtering to surface relevant social data in the right context."

One thing is certain: The consumerization of IT is continuing to have an impact on enterprise platform and software adoption, and we're likely to see more social media features finding their way into our business applications. If that helps companies work faster, collaborate more effectively, and reduce operating costs, it'll be hard to argue with the trend.

InstantDoc ID 139991

JEFF JAMES (jeff.james@penton.com) is industry news analyst for *Windows IT Pro*. He was previously editor in chief of Microsoft *TechNet* magazine, was an editorial director at the LEGO Company, and has more than 15 years of experience as a technology writer and journalist.

THE CONVERSATION BEGINS **HERE**

WINDOWS CONNECTIONS | Microsoft® Exchange CONNECTIONS | UNIFIED COMMUNICATIONS CONNECTIONS | SharePoint CONNECTIONS | SQL Server CONNECTIONS

BONUS TRACKS: > OFFICE 365 > EVALUATING / MIGRATING TO THE CLOUD

OCTOBER 31-NOVEMBER 3, 2011

LAS VEGAS, NV | MANDALAY BAY RESORT & CASINO

Be Here!

WinConnections and Microsoft will team up to deliver the WinConnections conference at Mandalay Bay Resort & Casino.

WinConnections will offer the most compelling sessions, thought-provoking keynotes, the most well-known speakers and glimpses into the future of IT computing from Microsoft and third-party experts.

Whether you're looking for future direction from Microsoft with Windows 8 or you need to make better use of Exchange, Lync, improve security, migrate systems, integrate with SharePoint, deploy better or develop your strategy for the cloud, WinConnections in Las Vegas is where you want to bring your team.

Make CONNECTIONS the CONFERENCE you bring your whole team to this year!

KEYNOTES

SCOTT GUTHRIE
MICROSOFT
CORPORATE VICE PRESIDENT, SERVER & TOOLS BUSINESS

KAMAL HATHI
MICROSOFT
GENERAL MANAGER SQL SERVER DEVELOPMENT TEAM

JEFFREY SNOVER
MICROSOFT
DISTINGUISHED ENGINEER

STEVE FOX
MICROSOFT
DIRECTOR, DEVELOPER AND PLATFROM EVANGELISM FOR SHAREPOINT

MARK MINASI
MINASI RESEARCH AND DEVELOPMENT

TONY REDMOND
TONY REDMOND AND ASSOCIATES

- **Train with 100+ Microsoft & Industry Experts at over 240 deep dive sessions.**
- **Attend cutting edge keynotes & keep your competitive edge.**
- **Network with Microsoft, industry experts, and colleagues.**
- **Attend the co-located event sessions at no extra charge.**

QUESTIONS ANSWERED • STRATEGY DEFINED • RELATIONSHIPS BUILT

EARLY BIRD DISCOUNT!

Register by September 19th and book a minimum of three nights at Mandalay Bay and you'll receive a $100 Mandalay Bay Gift Certificate and save $100 off conference registration!

FOLLOW US!
twitter.com/winconnect

FIND US!
facebook.com/winconnections

WINCONNECTIONS conference and expo

REGISTER TODAY! | www.WinConnections.com | 800.438.6720 • 203.400.6121

- Deciphering PKI
- Exchange Autodiscovery
- IT Security

LETTERS@WINDOWSITPRO.COM

Deciphering PKI

I just read Russell Smith's excellent article, "Deciphering PKI" (May 2011, InstantDoc ID 129847). I have one question about it. When does a client get a private key, which is used to encrypt the message digest, decrypt messages, and sign messages?

—Robert Mikołajczyk

Thanks for your message. I'm glad that you found the article useful. If I understand correctly, you want to know when a client receives a certificate to work with secure messaging in a program such as Microsoft Outlook. Users must either request or be assigned a certificate for use with secure messaging. This is usually done through an internal PKI. The user's email client then has to be configured to use the certificate for secure messaging. You can find more information about the infrastructure required to support secure messaging in Outlook 2010 in the Microsoft article "Plan for e-mail messaging cryptography in Outlook 2010" (technet.microsoft.com/en-us/library/cc179061.aspx).

—Russell Smith

Exchange Autodiscovery Questions

I have a few questions regarding John Savill's FAQ, "How can I quickly verify that my Exchange autodiscovery is working?" (June 23, 2011, InstantDoc ID 139558):

1. In John's examples, he shows both http:// and https://. I'm assuming he means just https:// and not http://. Correct?
2. If you create an "A" record for the autodiscovery, do you also have to have an SSL for it? That's assuming we don't have a wildcard SSL installed (which most of our clients do not). Or does the device know to ignore an SSL error and proceed?
3. What about internally? I have a few clients who can't open Outlook and have it automatically discover its settings (in a domain). Can/should we add an "A" pointer in the internal DNS for autodiscovery, and will that fix that problem? (We can manually put in the settings for Outlook and it works fine, just not autodiscovery internally in the domain.)

—Shawn Lemay

Good questions, Shawn.

1. *Yes, it is always https. Sorry about the typo.*
2. *Yes, you would typically need a certificate for the autodiscovery unless you have a wildcard normally. This scenario is explained in detail at technet.microsoft.com/en-us/library/bb310762.aspx. There is a way to just use one as described at technet.microsoft.com/en-us/library/bb310764.aspx. However, certificates are typically cheap these days, so purchasing an additional one for autodiscovery is fine for most clients. The more services an organization has on the web, the more attractive a wildcard certificate gets. They cost only a few hundred dollars, and most Microsoft services work with a wildcard certificate today.*
3. *Yes, you would have an autodiscovery on the internal DNS domain, and a separate autodiscovery for the Internet-based clients.*

I hope these answers help.

—John Savill

The Weak Link in IT Security

Jeff James has an excellent message in his article, "Are Users the Weak Link in IT Security?" (June 22, 2011, InstantDoc ID 139572). This is something we'll need to address in the near term with my employer. Please revisit this topic in future articles!

—Peet Rapp

InstantDoc ID 139973

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

Paul Thurrott...

. . . he's not in Microsoft's pocket, but now he can be in yours.

The independent voice for IT enthusiasts

Paul Thurrott delivers news, tips, commentaries, and reviews on Microsoft technology – from gaming to mobile to servers to software, and coverage of Microsoft competitors in between. Get daily updates without reaching farther than your pocket.

Download your
Paul Thurrott: PocketTech app today

windowsitpro.com/mobile-apps

Available for iPhone | Windows Phone 7 | Android

Thurrott

"Microsoft announced that support for Windows XP would finally expire in 1,000 days, allowing the software giant to continue its campaign to get customers off of the decade-old OS."

XP Support Expiring, Intune 2.0, Windows 7 Momentum, Windows Phone 7 Lack of Momentum, MDOP 2011 R2, iPad Imitators, and Simplified OSs in Apple's Lion and Windows 8

As summer turns into fall, I've got one thing on the brain: BUILD, Microsoft's new Windows 8 developer show, scheduled for early September. But as I write this in the days leading up to BUILD, Microsoft was nice enough to accommodate with news from its annual partner show, Worldwide Partner Conference (WPC) 2011.

XP Support Expires in Less Than 1,000 Days

At July's WPC, Microsoft announced that support for Windows XP would finally expire in 1,000 days, allowing the software giant to continue its campaign to get customers off of the decade-old OS. (Microsoft is also trying to get its corporate customers to stop using the aging Internet Explorer—IE—6.0 browser, which still ships with XP.) Microsoft offers many avenues for customers to migrate from XP to Windows 7, but given the partner focus at WPC, it's not surprising that the company chose to focus on solutions with a partner component. And the key solution that meets both those criteria is Windows Intune. (I wrote about Intune in "Windows Intune Brings PC Management Into the Cloud," May 2011, InstantDoc ID 129945.)

Beyond the basics, Intune offers some interesting benefits for organizations that decide to standardize PC management in the cloud. One of those benefits is a fully licensed copy of Windows 7 Enterprise for each managed PC. But when you consider that Windows 8 will ship before the 1,000 days is up (Windows 8 is due by mid-2012), you might wonder if you should wait for *that* release—certainly, some companies will be partway through a Windows 7 migration when Windows 8 hits. Are there any issues with having both Windows 8 and Windows 7 in the same environment?

As it turns out, no. Last month's preview of the new Windows 8 Start screen provides a hint of why (see Need to Know, "Windows 8 Start Screen Revealed," August 2011, InstantDoc ID 136415). Microsoft told me previously that Windows 8 and Windows 7 PCs would coexist nicely in the same environment and would largely be seen as identical by various management solutions and by Active Directory (AD)—because they're largely identical under the covers, with both OSs even sharing the same hardware requirements, which is a first in the history of Windows. (In some cases, Windows 8 will require even less in the way of hardware resources than its predecessor.)

The biggest innovations in Windows 8 will be in the user experience, not the underpinnings. Because many corporations will choose to use the older, traditional Windows UI on Windows 8 as well, even that difference might not ultimately affect businesses for some time to come. So, yes—continue with your migration away from XP. It's old, insecure, less productive, and harder to manage. And you don't need to use Windows 8 as an excuse to wait.

Now in Beta: Intune 2.0

Speaking of Intune, the second major version of Microsoft's cloud-based PC management service for small-to-midsized businesses (SMBs) is now in broad public beta and will ship in final form by the end of 2011. Intune 2.0 will be familiar to anyone who's used the first version—both the admin interface and the client experience are similar. In addition, Intune 2.0 adds a crucial missing feature that many version 1.0 customers asked for: software distribution.

This is a big deal, and it means that anyone with admin privileges in Intune 2.0 can deploy MSI- and EXE-based software packages (Microsoft and third-party) to remote PCs. And although there's no direct link between Intune and Microsoft Office 365 (yet), Microsoft did point out that environments using both services can easily use the Intune software distribution feature to distribute the Office 365 desktop setup application, as well as Microsoft Office Professional Plus 2010, which is included with enterprise versions of Office 365.

Intune 2.0 isn't just about software distribution, though, and Microsoft is adding a couple of other interesting new features and a nice bit of fit and finish work to all the UIs. A remote tasks feature lets admins perform more IT tasks on remote PCs, including full and quick antivirus scans, restarting the PC, and updating malware definitions. A new read-only admin users type provides a finer-grained delegation capability, so you can provide some users with the ability to run scans and reports but not do anything destructive, such as edit or deploy policies. The license management functionality is extended to third-party software (compared with the first version, which supported only Microsoft software). Microsoft also talked up the partner story for Intune at WPC and introduced some new sales incentives, including quicker up-front payments for new Intune licensees.

Windows 7 Momentum

As of mid-July 2011, Microsoft had sold more than 400 million licenses for Windows 7, the company's latest desktop OS. Microsoft provided a rough chart that more or less demonstrates that Windows 7 is selling at a faster clip than XP was at the same point in its life cycle—which isn't surprising, because Microsoft has repeatedly claimed that Windows 7 is the fastest-selling version of Windows ever. I came up with a better comparison that puts Windows 7 in perspective: Apple claims that there are now more than 50 million Mac OS X users, and I think it's fair to say that Windows 7 is in use on more PCs than are all version of Mac OS X combined—not too shabby for a product that's only been in the market for 20 months.

Windows Phone 7, Um, Momentum

Headlining the WPC this year, Microsoft CEO Steve Ballmer said that in Windows Phone 7's first year, the new OS went from being "very small" to being . . . "very small." That's not a typo—it's a cute way of saying that Windows Phone hasn't experienced much in the way of market success yet. But with Nokia coming on board for the version 2.0 release, which is code-named Mango and will almost certainly be marketed as Windows Phone 7.5, many feel that the software giant will see great success in year two. I'm still on the fence, but I'll say this: Windows Phone, even in its version 1.0 incarnation, has the user experience and technical chops to take on the iPhone and Android—and when you see Mango, you realize that Microsoft has taken the lead for good. Will users follow? We'll see, but I hope so: This is a product line that deserves better success than it has found so far.

MDOP 2011 R2

Microsoft Desktop Optimization Pack (MDOP) is one of those toolkits that's poorly understood by the masses but hugely loved by and valuable to those who use it. It's basically available in two ways: as a benefit of Microsoft's Software Assurance (SA) volume licensing program and as an add-on for Intune, where users can subscribe to it for $1 per PC per month (in addition the regular per-PC subscription fee). In August 2011, MDOP received a small upgrade to MDOP 2011 R2, and the following applications were updated as part of that release:

- Microsoft BitLocker Administration and Monitoring (MBAM) 1.0 is picking up BitLocker administration and monitoring capabilities, with improved reporting.
- Microsoft Diagnostics and Recovery Toolset (DaRT) 7.0 gains a few new features, including remote boot, which makes it possible to boot this recovery environment on PCs in your environment without needing to physically visit them.
- Microsoft Asset Inventory Service (AIS) 2.0 provides an updated (and localized) UI and improved reporting, bringing AIS up-to-date with Intune 1.0's reporting capabilities.

Tablets? There's iPad and Then There's . . . Well, There's Nothing Else

It seems like a new Android-based tablet is released every week now, but none of them have taken off in the market in any appreciable way. And then there's the RIM BlackBerry PlayBook, which inexplicably shipped without an email app or any meaningful third-party support, and HP's TouchPad, which looks almost exactly like a 2010-era iPad but also comes without any third-party support to speak of. Even ThinkPad's creator, Lenovo, is getting into the game with a ThinkPad-branded tablet this year—but it runs Android, not Windows. What gives?

The simple fact is, there are no truly across-the-board compelling alternatives to the iPad yet—and to be honest, I don't see it happening until Windows 8 and a new generation of ARM-based competition appears in mid-2011. The issue isn't all that complex, it's just next to impossible for any of Apple's would-be competitors to overcome. Although it's possible and even easy for any one company to duplicate the iPad's look, feel, weight, thinness, and battery life, none of those are the real reasons that consumers buy iPads. Instead, people choose iPads because Apple offers the richest ecosystem, with the largest markets anywhere for online music, TV shows and movies, apps, podcasts, audio, e-books, and other content. There's just nothing like it anywhere else.

There's one dark horse you should know about, however. Online retailing giant Amazon.com is widely rumored to be prepping its own massive tablet launch, and that device could finally provide Apple with a serious threat. Amazon's tablet will run on Android, but it will also be backed by a trustworthy company that sells digital music, TV shows and movies, apps, e-books (Kindle), audio books (Audible), and other content—and that can also afford to undercut Apple on pricing.

Beyond Amazon, it's just a waiting game while Microsoft catches up. When Windows 8 ships next year, things might change. But until then, you're just treading water if you think that any tablet wannabe makes any sense at all. Today, it's all iPad. Tomorrow, maybe Amazon, and then Windows 8.

Toward a Simpler OS Future

After using the next version of Mac OS X—called Lion—and watching Microsoft's video demonstrations of the new Windows 8 Start screen, it's pretty clear that both OS makers are taking the simpler user experiences from their mobile OSs—iOS and Windows Phone 7, respectively—and bringing them to mainstream PCs. Apple will get there first—Lion will be broadly available well before you read this—but Microsoft's vision for Windows 8 seems more forward leaning, so it's a bit of a wash.

The move toward simpler user experiences is long overdue, but it will rankle power users the most. As with the Microsoft Office Ribbon UI before it, the Windows 8 Start screen is pretty but scary, especially for those of us who've spent the past several years honing our Windows skills. And not surprisingly, I'm seeing a lot of griping from power users in both the Windows and Mac camps who aren't too thrilled with this new direction.

But don't get distracted here. Simpler is always better, and although you can go too far, as Apple sometimes does (e.g., no Back button on the iPhone or iPad), the end result will be more approachable devices that serve a much wider audience. Fear not, power users. Your skills will always be required. But as with the rest of us, you might need to learn some new tricks when these new UIs go mainstream.

InstantDoc ID 139895

PAUL THURROTT (paul@windowsitpro.com) is senior technical analyst for *Windows IT Pro*. He writes the SuperSite for Windows (winsupersite.com), a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email), and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

Minasi

"Unless you're being paid by the hour, it's no fun to type GUIDs."

Finishing Up Your Windows PE Maintenance System

This alternative deployment strategy is easier to keep running

Last month, I began exploring how to create a more "fixable" deployment of Window 7 or Windows Server 2008 R2 than the one I shared in "Adding Windows PE to Your Windows 7 System" (May 2011, InstantDoc ID 129793). In this alternative strategy, you install the OS as before but change the 100MB "hidden" partition to 1000MB and add a bootable copy of WinPE both to that partition and to the Windows boot manager menu, solving the age-old "I'm trying to fix a non-bootable copy of Windows NT, but there's no such thing as an NT boot floppy to get my repairs started" conundrum. Last month, you started the process by wiping a target computer, creating the 1000MB partition, and installing the OS on the remaining space.

This month, you'll use the Windows Automated Installation Kit (WAIK) and ImageX to install WinPE onto the 1000MB partition, then use Bcdedit to add WinPE to the boot manager menu. If you've been following these columns, you'll find no surprises; you'll be using tools that you've seen before. In a sense, this is just a particularly useful application of previously covered power tools.

Boot up your freshly installed copy of Windows 7 or Server 2008 R2, surf over to www.microsoft.com/downloads, and pull down the latest version of the WAIK. (Do *not* download the newer "Supplement.") Install the WAIK.

Next, you're going to use ImageX to apply the WAIK's WinPE image (in WIM file format) to the 1000MB partition, which doesn't have a drive letter. Unfortunately, ImageX needs a drive letter before it can apply a WIM file, so you have to give the unlettered partition a drive letter before proceeding. You can use Diskpart, as I've described in earlier columns, or you can use the GUI by clicking Start, typing *diskmgmt.msc* into the *Search programs and files* field, and pressing Enter. Locate and right-click the unlettered 1000MB partition in the Microsoft Management Console (MMC) Disk Management snap-in. Choose *Change Drive Letter and Paths* and, in the resulting dialog box, click Add, then click *Adding the following drive letter*, choose the letter T, and click OK. Minimize the Disk Management snap-in but don't close it; you'll want to remove that drive letter once you have WinPE installed.

Next, click Start, All Programs, Microsoft Windows AIK, then right-click Deployment Tools Command Prompt, choose *Run as administrator*, and click OK at the UAC prompt. An elevated command prompt is now open at C:\Program Files\Windows AIK\Tools\PETools. In that folder are three folders named amd64, ia64, and x86, each containing an entire copy of WinPE—one for standard 64-bit systems, one for the nearly nonexistent Itaniums, and one for standard 32-bit systems. If you're adding WinPE to a 32-bit Windows 7 system, type *cd x86* and press Enter; if you're adding WinPE to a 64-bit Windows 7 or Server 2008 R2 system, type *cd amd64* and press Enter. Image WinPE onto your T drive with the command

```
imagex /apply winpe.wim 1 t: /verify
```

You should see the message *Successfully applied image* and a report of the elapsed time. WinPE is on your hard disk, but your OS doesn't know how to boot from it. To fix that, create a second OS entry from your one current one with the following command. (Type it right at the Deployment Tools Command Prompt.)

```
bcdedit /copy {current} /d "Boot WinPE"
```

Bcdedit will report the GUID of the newly created OS entry:

```
The entry was successfully copied to {8868422c-79b7-
  11e0-964b-c25a31d9e8b7}
```

Copy that GUID—the hex value between the curly braces—into your clipboard by right-clicking the command prompt window and choosing "Mark," then highlight the GUID and press Enter. (You'll want to do that because the next four commands require you to enter that GUID, and unless you're being paid by the hour, it's no fun to type GUIDs.) Then, type these four commands, replacing *{GUID}* with your actual GUID value by right-clicking in the command window and choosing Paste:

```
bcdedit /set {GUID} osdevice partition=t:
bcdedit /set {GUID} device partition=t:
bcdedit /set {GUID} winpe yes
bcdedit /set {GUID} detecthal yes
```

Finally, return to the Disk Management snap-in and remove the letter from the 1000MB partition by right-clicking it, selecting *Choose Drive Letter and Paths*, highlighting T, clicking Remove, and assuring Windows that you do, indeed, want to un-letter the partition. Congratulations, you've now built a copy of Windows that is a trifle easier to keep running. Enjoy it!

InstantDoc ID 139826

MARK MINASI (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 30 books, including *Mastering Windows Server 2008 R2* (Sybex).

Penton Marketing Services
WE KNOW YOUR CUSTOMERS
powered by eyetraffic

Do you know what is being said about your company online?

DO YOU KNOW WHAT IS BEING SAID ABOUT YOUR COMPETITION?

We do.

Do you have time to warm prospects towards a sale?

DO YOU HAVE THE RESOURCES TO RESPOND QUICKLY TO PROSPECT BEHAVIOR?

We do.

Announcing, smart marketing for the technology industry.

We target the tough questions.

Windows IT Pro
SQL Server magazine
SharePoint Pro CONNECTIONS
DevProConnections
System iNetwork

Penton Marketing Services offers a full range of marketing products that leverage our deep industry knowledge and customer relationships. From product launch to the final sale—put our years of experience to work for you.

FOR MORE INFORMATION:
PentonMarketingServices.com
800 553 1945

Otey

"Because Intune is cloud-based, it isn't limited to monitoring a single location."

Reasons to Use Windows Intune

Simple cloud-based management and security for desktops in a cloud model

Windows Intune could be the first cloud-based application that businesses really adopt. Intune provides simple cloud-based management and security for the desktop PCs in your environment. In its early stages, Intune is no replacement for System Center, but all indications are that Microsoft will vastly expand the capabilities of future Intune versions. Here are the top 10 benefits provided by Windows Intune.

10 **Price**—Intune possesses a client component, but it's sold as a service. The current price for Intune is $11 per PC per month. This price might seem a bit high for small-to-midsized businesses (SMBs), but it also includes an upgrade to Windows 7 Enterprise edition. You can get a free 30-day trial of Intune for up to 25 PCs from Microsoft's website at www.microsoft.com/windows/windowsintune/pc-management-how-to-try-and-buy.aspx.

9 **Components**—Intune is comprised of a client agent and an administrative console. The administrative console is web-based and requires Silverlight 3.0. The client agent lets you manage desktop PCs; it comes in an .msi file that's signed with a certificate, making it unique to each customer. It can be downloaded from the Intune site or distributed through Group Policy.

8 **Malware protection**—The Intune client takes advantage of the same Microsoft Malware Protection Engine that's supplied with the well-regarded Microsoft Security Essentials (MSE) product. The Intune malware engine protects against both viruses and spyware, and it shares the same malware definitions and research that MSE uses.

7 **Centrally managed updates**—Like Windows Server Update Services (WSUS), Intune can deliver software updates to Windows as well as Microsoft applications. Unlike WSUS, which works over your network infrastructure, Intune delivers those updates from the cloud (i.e. the Internet). Intune supports auto-deployment rules as well as customized installation and notification of the updates deployed.

6 **Centrally managed security policies**—Although Intune isn't integrated with Active Directory (AD), administrators can still use it to distribute security policies to all Intune-managed PCs. Intune lets the administrator control updates, firewall settings, and endpoint protection policies. If these PCs are also managed by AD, then AD's Group Policy settings will take precedence.

5 **Remote assistance**—Intune can provide remote assistance. A desktop icon on the Intune client lets the desktop user request remote assistance, which sends an alert to the Intune administrative console; these requests can also be sent through email. The administrator can then respond to the request, which starts a Microsoft Easy Assist session where the administrator can chat, send files, or share the desktop with the end user.

4 **Tracking hardware and software inventory**—The Intune administrative console lets you see the basic hardware configuration of each managed PC as well as the software installed on the client system. Inventory scanning lets administrators find unapproved and unlicensed applications. In case you were wondering, Microsoft can't access your Intune license reports.

3 **Reporting**—Intune delivers Updates, Software, and Licenses reports. Each of these reports allows custom filtering and reporting criteria. The Updates report shows the status of the patches and updates deployed. The Software report lists installed applications. The Licenses report compares deployed software to your current license agreements. Reports can be exported to HTML or to CSV files for importing to Microsoft Excel.

2 **Desktop monitoring**—One of the primary benefits that Windows Intune provides is the ability to monitor the health of the Intune-managed desktops. Intune uses the Microsoft System Center Operations Manager 2007 R2 agent in conjunction with the Windows Intune Monitoring agent. The Ops Manager agent reports on hardware and software health, and the Intune Monitoring agent reports on the status of the Intune agents themselves. Alerts are sent to the Intune administrative console.

1 **Manage multiple accounts**—Because Intune is cloud-based, it isn't limited to monitoring a single location. The Intune Multi-Account Console provides a summary view of the current status of multiple customer accounts, which is a great feature for consultants working with different customers. The Multi-Account Console lets you filter accounts based on their status as well as drill down into the specific status of each account.

InstantDoc ID 139793

MICHAEL OTEY (motey@windowsitpro.com) is senior technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).

Deuby

"Token bloat won't affect just one of your users when it hits: It will affect a lot of them."

The Care and Feeding of the Active Directory Security Access Token

Beware token bloat!

When we talk about enterprise computing, and enterprise identity, we usually talk in terms of large-scale system architectures. But architectures can scale from enormous to minuscule—down to the level of packets on the wire. In my past few columns, I've spoken about some of the big identity issues we're dealing with today, such as securely connecting your enterprise to that great big service station in the sky (aka the cloud). This month, I'd like to talk about something on the other end of the identity scale, something down near the atomic level in IT terms: the Active Directory (AD) security access token. This little mote controls authorization in an AD domain, and if you don't pay attention to it, you might be setting yourself up for some big problems.

A Token in a Ticket

The Kerberos security protocol is the bedrock upon which AD builds practically everything else. Strictly speaking, the Kerberos protocol handles only authentication (securely identifying a user's identity on a computer network). With the introduction of Windows 2000, Microsoft extended the Kerberos protocol to also handle authorization (determining whether a user has rights to access a resource). At the time, Microsoft was criticized for extending existing standards for its own purposes and causing interoperability problems with other Kerberos systems. In this case, the Kerberos standard does provide for extensions by making a user-defined field—a placeholder—in the ticket-granting ticket (TGT) called the Privilege Attribute Certificate (PAC). Microsoft stores the security access token in the PAC field of the Kerberos ticket to handle authorization.

How is the access token created? When a user successfully authenticates to an AD domain, the Kerberos Key Distribution Center's Authentication Service queries its local directory service and the closest Global Catalog to determine what groups the user is a member of. It then generates an access token that contains those groups and their SIDs, and the user's name and SID, and adds it to the TGT.

Token Bloat

The size of the PAC field and the access token it holds is finite; the field doesn't stretch to fit a large access token pushing up against the PAC's limits. Therefore, the limit to the number of groups a user can be a member of is about 1,015. This is because the PAC can hold only 1,024 SIDs, minus a varying number of well-known groups that the Local Security Authority (LSA) adds to the access token. (For more information, see the Microsoft article "Users who are members of more than 1,015 groups may fail logon authentication" at support.microsoft.com/kb/328889.) That limit might sound very large, but users can run up against this access token limit with as few as 270 groups, and begin to feel its effects long before they reach the limit. This situation is known as token bloat, and it won't affect just one of your users when it hits: It will affect a lot of them.

Why? Because other mechanisms, such as RPC and HTTP, rely on the MaxTokenSize registry value (HKEY_LOCAL_MACHINE\SYSTEM\CCS\Control\Lsa\Kerberos\Parameters) when they allocate buffers for authentication. By default, MaxTokenSize is 12,000 bytes; if a user is a member of more than 120 groups, he or she might begin to experience slow logons and other erratic behavior, and users with greater numbers of groups in their access token will encounter authentication errors and Access Denied authorization errors.

> Using a deeply nested group structure—though it might be convenient from an organizational viewpoint—will increase the average size of the user's access tokens.

The MaxTokenSize value can be adjusted upward to accommodate more groups. (For more information, see the Microsoft article "How to use Group Policy to add the MaxTokenSize registry entry to multiple computers" at support.microsoft.com/kb/938118.) However, OSs since Windows Vista and Windows Server 2008 will automatically adjust MaxTokenSize upward to compensate for greater group membership. But this is just a Band-Aid on the problem; users will still experience the slowdown effects of a large access token, and the 1,015-group limit cannot be exceeded regardless of how high you manually set MaxTokenSize.

It's important to keep in mind that when a user's group membership is enumerated to create the access token, it includes all transitive group memberships as well. This means that using a deeply nested group structure—though it might be convenient

from an organizational viewpoint—will increase the average size of the user's access tokens. For example, if you're a member of the Muleshoe Users security group, which is a member of the Bailey County Users group, which is a member of the Texas Region group, which is a member of the US Region group, you already have four group SIDs in your access token.

There's a further consideration in this debate about token size. Different group types take up varying amounts of space in the PAC. Domain local groups take 40 bytes to store in the PAC, but global groups and universal groups take only 8 bytes per group. So, if you've been following group-nesting guidelines to focus on domain local groups, you'll see token-bloat problems sooner than in a domain that uses global and universal groups.

Another place token bloat will bite you is related to Microsoft SharePoint. Starting with SharePoint 2007, security groups—not just distribution lists (DLs), which don't have a SID—are required to configure permissions to SharePoint resources. The easiest solution, and one I'm sure many companies have implemented, is to simply turn all DLs into security groups. This is potentially a nightmare—first, because you probably haven't managed or organized your DLs in the same way you've organized your security groups for access control, and second, because it will dramatically increase the size of your users' access tokens when all these DLs show up in them. How many mail DLs are you a member of? Do you even know?

A Crash Token Diet

You can make some temporary fixes to hold things together, but to really fix token bloat you need to adopt a number of best practices in group management and object lifecycle management. Let's look at the quick fixes first.

First, consider bumping MaxTokenSize up to its maximum setting of 64K (i.e,. 65535). This doesn't solve your token-bloat problem, but it will stave off authentication failures in RPC and HTTP due to MaxTokenSize not being large enough. The Microsoft article "How to use Group Policy to add the MaxTokenSize registry entry to multiple computers" (mentioned earlier) will show you how to use Group Policy to set this value for multiple users.

Second, the easiest way to quickly look at your own group membership is to use the Whoami command-line utility, which is included in Windows. (Whoami will also show information about the current user on the local system, so it's a very handy utility if you need to confirm who you're logged on as.) For group membership, you'll want to use the /groups parameter, which will enumerate all the direct and transitive groups—and their SIDs—that you have in your access token. You can run this command only locally, however.

Third, Tokensz (in the Microsoft Download Center at www.microsoft.com/download/en/details.aspx?id=1448) will check a user's MaxTokenSize setting, and the /calc_groups option will list a user's groups. With some creative scripting, you could run Tokensz against all (or a sampling of) your users to discover potential trouble spots. Ntdsutil has a function, Group Membership Evaluation, that you can run against an individual user to get detailed information about his or her access token. In addition to listing the user's groups, it will also show SID history (which increases access token size) and group type, so it's a good way to dive a little deeper into the most affected users.

Fourth, another quick fix is to look at your most severely affected users and see if you can simply remove them from groups they no longer need to be a part of. This is a classic symptom of poor account and object lifecycle management, because it's much easier to add someone to a group when they're needed than to remove them from the group when they're not. With information from Group Membership Evaluation, you could minimize a user's domain local groups to free up access token space.

Microsoft has a detailed document about the token-bloat problem—"Addressing Problems Due To Access Token Limitation" (www.microsoft.com/download/en/details.aspx?displaylang=en&id=13749)—to step you through remediation. To really solve the problem, however, you have to take a more strategic view of how you manage your security groups. These are the areas you should focus on:

- Minimize nested groups—There's nothing wrong with nested groups; just don't get carried away with them. It's not uncommon to find circular nesting several layers deep, and that will drive you crazy in a hurry.
- Use domain local groups as the final group into the resource, and nowhere else—Promote domain local groups to global groups and universal groups where appropriate. You'll need to study the pros and cons of the different group types, especially if you have a multi-domain forest, because each has advantages and disadvantages.
- Get on top of your group lifecycle management—This is a widespread problem in AD installations. There's usually an urgent need to create groups, add users, and populate resources for new projects. There's rarely that same urgency to remove users from groups, groups from server ACLs, and actually delete groups unless it's driven by information security and a clear lifecycle plan. Products such as Imanami's GroupID specifically focus on group lifecycle management; the challenge in this approach is getting IT management to pay for a need that's important but not urgent.
- Limit your account administrators—The fewer individuals that can create groups, the less chance you'll have too much group creation.

Are You Vulnerable?

Token bloat is a common problem in larger AD installations, especially ones that have been around for a while and that don't have good group lifecycle management. If you fit into this category, use this article's tools to look at your user community and head off token bloat before it begins.

InstantDoc ID 139827

SEAN DEUBY (sean@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine*, and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.

- iSCSI
- Exchange Server
- Kerberos
- Windows Firewall
- Hyper-V

ANSWERS TO YOUR QUESTIONS

Q: What command can verify that the Hyper-V Volume Shadow Copy Service (VSS) writer is registered?

A: Backing up a running database requires a process called quiescence. This "quieting" of the database creates a point in time from which a backup job can begin its activities. That point in time allows the database to continue operating during the backup. Any changes that occur during the backup are then incorporated at the job's completion.

A Hyper-V Virtual Hard Disk (VHD) file is much like a database in that changes are constantly occurring inside the virtual machine (VM). Thus, backing up a VHD from the host requires the same quiescence process. This process is enabled through the Microsoft Volume Shadow Copy Service, and requires a specific VSS writer for Hyper-V.

The Hyper-V VSS writer is installed with the installation of the Hyper-V role, but it isn't automatically registered with VSS. Registering the writer requires navigating to HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion, adding the keys WindowsServerBackup\ApplicationSupport{66841CD4-6DED-4F4B-8F17-FD23F8DDC3DE}, and then adding a REG_SZ value of Application Identifier with the value of Hyper-V.

You can then verify that the Hyper-V VSS Writer has been registered by entering the command

```
vssadmin list writers
```

You should see the Microsoft Hyper-V VSS writer in the resulting list.

—Greg Shields

InstantDoc ID 139638

Q: Can I restore a Virtual Hard Disk (VHD) to a different Hyper-V server?

A: Yes, but not without the occasional hiccup. A Hyper-V VHD can be restored to an alternate server using any backup application. Hyper-V virtual machines (VMs) restored in this way might experience problems as they power on. Network adapter names might not be consistent with the new host, or machine configuration conflicts might exist in the VHD's saved state data.

If you need to resolve a network adapter name inconsistency, launch the Hyper-V Management Console on the server where the VHD has been restored and open the Virtual Network Manager. Rename the restored VHD's network adapter to give it the same name as the adapter that's being used on the host. Then, start the VM.

If the VM still won't start, delete any saved state files by right-clicking the restored VM and selecting Delete Saved State. Occasionally, this step won't delete the necessary files. If it doesn't, locate the folder where the VHD has been restored and manually delete any existing .BIN or .VSV files.

—Greg Shields

InstantDoc ID 139636

Q: I have a Hyper-V virtual machine (VM) that's frozen, how can I dump its memory for troubleshooting?

A: If you have a frozen VM (or any VM or snapshot) , and you want a memory dump, use the vm2dmp.exe utility that's provided by Microsoft. To dump out a running VM's memory, use the command

```
vm2dmp.exe -vm <Virtual Machine name>
  -dmp <dump file name and location>
```

You can also get dumps from VM snapshots and state files by using the -snap and -vsv switches, as described on the download page.

—John Savill

InstantDoc ID 139760

Q: I installed the System Center Service Manager web portal on my management server, but the website is missing formatting and graphics. What do I do?

A: When you install the SCSM Management Server, you have to enable the .NET Framework 3.51 framework and role services of IIS. You don't need to install the Static Content role service for the management server. However, this is required for the web portal—without it, your web portal will be missing images.

You therefore need to start Server Manager, navigate to Web Server (IIS), and under Role Services, click Add Role Services and enable Static Content. Once you've installed Static Content, when you refresh the web page it will look correct.

—John Savill

InstantDoc ID 139498

Jan De Clercq | jan.declercq@hp.com
William Lefkovics | william@mojavemediagroup.com
John Savill | jsavill@windowsitpro.com
Greg Shields | virtualgreg@concentratedtech.com

Q: I accessed my Microsoft Outlook account through a web browser, and now in Outlook I get an error message that a UID doesn't comply with the IMAP Standard. What happened, and how do I fix it?

A: If you use Outlook for IMAP access to retrieve email from an IMAP server, and access the same account from another source (especially through web access) while Outlook is connected to that account, you might face a series of annoying errors when you return to Outlook. Companies that employ IMAP as their primary email-access protocol on their corporate messaging servers and allow employees multiple access methods (e.g., web mail, other IMAP clients) along with Outlook will probably see these pop-ups. These errors focus on the sequence of unique identifiers (UIDs) assigned to IMAP messages. These UIDs aren't the same as the SMTP message IDs; these are specific to IMAP. The Outlook errors come in pairs. The first error states *The UID of a message changed unexpectedly. This typically indicates a server bug. Your program may not function properly after this.*

The text of the second error is *Your server reported a UID that does not comply with the IMAP Standard. This typically indicates a server bug. Your program may not function properly after this.*

The text of these errors hasn't changed in 10 years (maybe more). It doesn't typically indicate a server "bug," but certainly errors, corrupted content, or poor implementation on the server could lead to such problems on a client. Outlook just doesn't handle this situation well. There's no way to access Outlook again until these errors are cleared. A bigger problem occurs if you were very active with the web client while Outlook was open to that account. The UID errors might pop up for every message you highlight in Outlook that was changed or opened in another client. If you deleted 20 messages through the web interface and Outlook was open with IMAP access to that mailbox, you could potentially be clearing 40 UID error notifications when you return to Outlook.

Outlook synchronizes folders on the IMAP server when the IMAP account is first accessed in Outlook after startup. These errors seem to arise when Outlook is expecting something that's no longer there or has been altered by a different source. When you click OK on the errors, Outlook accepts the change, essentially resetting Outlook's expectation of UID order, so you'll be back to normal. Restarting Outlook will also resynchronize the IMAP folders. If you initiate protocol logging on the Outlook client, you'll be able to identify the error within the logs, but the log doesn't provide insight to alleviate the problem. (For information about initiating protocol logging, see "Troubleshooting IMAP Connectivity in Outlook 2003," InstantDoc ID 96355.)

Implementation of IMAP is described in "RFC 3501: Internet Message Access Protocol—Version 4rev1," tinyurl.com/3fbr9r. Section 2.3.1.1 of RFC 3501 explains unique identifiers and how they should be handled on an IMAP server. Most importantly, "the unique identifier of a message MUST NOT change during the session." Outlook doesn't do a good job of handling subtle IMAP server violations of the UID aspect of RFC 3501.

For Outlook 2002, Microsoft released a support article advising users to remove the IMAP account and recreate it (see "OL2002: Error Message: 'Your Server Has Reported a UID Which Does Not Comply with the IMAP Standard,'" tinyurl.com/3lvqweq). This process really isn't necessary if the cause of the UID errors is simply making changes to the IMAP content from another source while Outlook is accessing the account. After you clear the UID errors, you can continue with Outlook as before.

Remember the anecdote about the patient who tells the doctor, "It hurts when I do this," and the doctor replies, "Don't do that"? Well, the same principle applies here: Don't access a mailbox with web access while Outlook has an open connection to that mailbox using the IMAP client protocol, and you won't encounter this problem. If you do leave Outlook with IMAP access to a mailbox and access that mailbox from an alternate client, you might have some UID errors to accept when you get back to Outlook. The best solution might be to close Outlook if you're using IMAP and expect to access your mailbox with other clients.

—William Lefkovics

InstantDoc ID 139684

Q: What Diskpart commands will prevent you from creating a misaligned Virtual Hard Disk (VHD)?

A: Physical hard drives break up their data by blocks, and virtual machines (VMs) do the same. When a VM's partitioning of those blocks doesn't match the partition boundaries on the host, the virtual disk is considered misaligned. That misalignment inappropriately overlays the virtual disk's blocks atop the host's physical blocks, forcing more physical blocks to be read from or written to than should be necessary.

New virtual disks can be created with the proper alignment using the Diskpart command. First, boot the VM into a version of WinPE that includes support for a command prompt. Then enter the following commands to create an aligned partition:

```
diskpart
list disk
select disk <diskNumber>
create partition primary align=32
exit
```

Once the aligned partition has been created, you can format the disk normally.

—Greg Shields

InstantDoc ID 139633

Q: Is there a way to control what's prefetched by Windows OSs?

A: Normally, when Windows boots, it "prefetches," loading commonly used files used for applications and for the boot process into memory. You can change this prefetch behavior, disabling it for everything or for applications or boot files.

1. Start the registry editor (regedit.exe).
2. Move to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters.
3. Double-click EnablePrefetcher.
4. Set it to 0 to disable, 1 to fetch only application files, 2 to fetch only boot files, or 3 to fetch application and boot files (the default).
5. Click OK.

This setting will take effect at next reboot.

—John Savill

InstantDoc ID 139647

Q: Do I have to update Hyper-V Integration Services after a Server 3008 R2 SP1 install?

A: Hyper-V's Integration Services are a necessary installation into most Hyper-V virtual machines (VMs). Installing Integration Services adds necessary drivers and services that let the VM perform its best on a Hyper-V host.

Windows Server 2008 R2 SP1 includes important updates to these drivers and services, requiring them to be updated after SP1 is installed to a Hyper-V host. Perform this update by clicking Action, Insert Integration Services Setup Disk, then Install Hyper-V Integration Services in each VM's Virtual Machine Connection. This process can be automated using System Center Virtual Machine Manager (SCVMM).

—Greg Shields

InstantDoc ID 139634

Q: Why is time synchronization between Windows machines critical in an Active Directory (AD) environment? How important is this for Kerberos authentication? What service controls time synchronization on Windows machines?

A: Windows AD needs timestamps for resolving AD replication conflicts and for Kerberos authentication. Kerberos uses them to protect against replay attacks—where an authentication packet is intercepted on the network and then resent later to authenticate on the original sender's behalf.

When a Windows server receives a Kerberos authentication request, it compares the timestamp in the request with its local time. If the difference between the local time and the timestamp is too big, the authentication request is rejected and Kerberos authentication fails. The allowed time skew can be configured using the *Maximum tolerance for computer clock synchronization* GPO setting (located in the Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy GPO container). It determines the maximum time skew (in minutes) that Windows will tolerate between client and a server clocks in a Windows Kerberos environment. Setting the time skew too high creates a higher risk for replay attacks. The default setting is 5 minutes.

The service responsible for time synchronization between Windows clients and AD domain controllers (DCs) is the Windows Time service (W32time.exe). All Windows machines, starting with Windows 2000 and Windows XP, have the W32time service installed by default. The time service will automatically perform time synchronization at machine startup and at regular intervals (by default, every 8 hours). In an AD forest, the machines use a time hierarchy that follows the following rules:

All client machines and member servers use their authenticating DC for time synchronization.

All DCs in the same domain use the DC with the primary DC (PDC) emulator Operations Master role as their DC for time synchronization. In an AD domain hierarchy, the PDC emulator DCs of a child domain synchronize time with the PDC emulator in its parent domain.

The PDC emulator DC in the root domain of the AD forest is the authoritative time source for the forest. The PDC emulator can also be manually set to synchronize with a time source on the Internet. Many organizations rely on an external time source for time synchronization. In organizations that have a Windows forest that's geographically spread out, it's recommended to configure an external time source for each region instead of using a single time source for the entire forest.

Microsoft provides two tools to configure and diagnose the Windows Time service: net time and w32tm. Both allow you to configure the time hierarchy to use the Windows defaults (as explained above) or to use specially designated time servers.

Net time can be used to configure the time service and the synchronization hierarchy. The following net time command will change the time server on the local machine to mytimeserver.hp.com:

```
Net time /setsntp:mytimeserver.hp.com
```

w32tm can be used to diagnose and configure the time service. For example, to monitor and analyze the time synchronization in the hp.com domain, type

```
w32tm /monitor /domain:hp.com
```

In Windows Server 2003, Microsoft added a new section in the GPO settings to configure the Windows Time Service. You can find it under Computer Configuration\Administrative Templates\System\Windows Time Service. The time service's configuration data are kept in the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\w32Time.

For many more Windows time service operation and configuration details, read the Microsoft article "Windows Time Service Technical Reference," tinyurl.com/3dp5gfc.

—Jan De Clercq

InstantDoc ID 139630

Q: I have an ASP.NET site. I've noticed that the first time I access the site, it's slow, but then it's faster. If I don't use it for a while, the first access is slow again. How can I stop this slowness?

A: IIS uses something called Just In Time (JIT) compilation, which compiles ASP.NET pages as they're accessed the first time. Then this compilation is cached in the AppPool, so subsequent accesses are fast. If a site isn't accessed for a long time, this cached compilation is recycled, freeing up resources. But this means that the next access requires compilation again. You can change the settings so the recycling doesn't occur:

1. Start the Internet Information Services (IIS) Manager.
2. Select <server>, Application Pools.
3. Right-click the application pool for the site you want to change. Select Advanced Settings.
4. Change both the Idle Time-out (minutes) entry under Process Model and the Regular Time Interval (minutes) under Recycling to 0 and click OK.

You can now right-click the pool and select Recycle to force a recycle using the new values.

Access the site in a browser to force the initial compilation, which will no longer be recycled, thanks to your new settings.

—John Savill

InstantDoc ID 139561

Q: I'm trying to start a Hyper-V virtual machine (VM) but I get an error stating that a .bin file couldn't be created in the folder of the VM. What should I do?

A: When a VM is started, a binary file (.bin) is created in the VM's folder, equal in size to the current memory allocation. (It'll change if the VM uses dynamic memory, and you might see a small difference).

If you receive an error when trying to start a VM stating that Hyper-V couldn't create the BIN file, check your disk space and make sure you have enough to create a BIN file equal to the memory of the VM. If you're having this problem, you really should look to add more disk space or move VMs, because you don't want to be running your storage this full.

—John Savill

InstantDoc ID 139494

Q: How can I quickly verify that my Exchange autodiscovery is working?

A: The first step is to make sure there is an autodiscover host (A) record for your domain that points to the server hosting autodiscovery. Use the command Nslookup. For example,

```
nslookup autodiscover.savilltech.net
```

Next, try to access your autodiscovery service using a web browser. The URL you should use is http://autodiscover.<your domain>/autodiscover/autodiscover.xml. You should receive some XML with an error in it; that's correct. If you don't get XML, you need to troubleshoot your discovery service in Exchange.

—John Savill

InstantDoc ID 139558

Q: Do I need to change anything if I install Windows 7 to a solid state disk (SSD)?

A: No manual changes are required when installing to an SSD. The OS will detect the presence of the SSD and automatically make changes, such as disabling automatic defragmentation jobs. You can make some tweaks for maximum performance:

- Make sure you have the latest firmware for your SSD and motherboard.
- Wipe the SSD using a utility to write 0's to all parts of the disk, which cleans the drive. The command

```
diskpart clean all
```

  will also achieve this.
- Use AHCI mode in the BIOS for the controller.
- Use the latest storage drivers.

—John Savill

InstantDoc ID 139644

Q: I'm trying to deploy Forefront Endpoint Protection (FEP) using System Center Configuration Manager (SCCM) 2007 using a custom advertisement, but it isn't working. Why not?

A: When the FEP server components that integrate with SCCM are installed, a package, a program, and an advertisement are automatically created to enable deployment of the FEP client, which can be set to download to a cache then execute. If you create your own advertisement that allows installation from the distribution point, the FEP client install will fail.

Because FEP is a security component, it must be installed from the local cache, so make sure you enable *Download content from distribution point*. Run locally under the Distribution Points tab of the advertisement.

—John Savill

InstantDoc ID 139753

Q: I'm using a third-party firewall service on Windows 7 that disabled the Windows Firewall for all profiles. Should I also disable the MpsSvc service that enables the Windows Firewall?

A: No. While MpsSvc does enable Windows Firewall functionality, it's also used for other functionality, such as IPsec. Not only is disabling this service not recommended, it's also not supported by Microsoft.

—John Savill

InstantDoc ID 139657

Q: I installed the Microsoft iSCSI Target but clients can't connect, even though I've created iSCSI Targets on the installation. What's wrong?

A: When you create an iSCSI Target with the Microsoft iSCSI Target software, you create devices and assign them to an iSCSI Target. You also need to tell the target which clients are allowed to connect—which by default is no one. Select the properties of the iSCSI target and, on the iSCSI Initiators tab, click Add and select the IQNs of the clients who are allowed to connect. The IQNs of clients that have tried to connect in the past will be displayed, or you can manually type the IQN of the allowed clients. The clients should now be able to connect.

If you're unsure of the IQN of an iSCSI Initiator (the client), launch the iSCSI Initiator Administrator Tool application on the client. Its IQN is shown on the Configuration tab.

—John Savill

InstantDoc ID 139654

Q: How can I restore a single file or folder from a Virtual Hard Disk (VHD) using Windows Server Backup (WSB)?

A: WSB is Windows' native solution for backing up files, folders, and entire Hyper-V VHD files. When WSB is configured on a Hyper-V host, VHDs can be backed up as single files. This enables single-file restoration of entire virtual machines (VMs), but makes restoring individual files and folders challenging.

To restore a single file or folder from a VHD that's been backed up using WSB, first restore the VHD to an available server. Once it's restored, launch Disk Management on that server and select Action, Attach VHD. Point the wizard that appears to the restored VHD and choose OK. Then, right-click the now-attached VHD and select Explore. A Windows Explorer window will appear, allowing you to locate and restore the file or folder. Return to Disk Management and select Detach VHD when complete.

—Greg Shields

InstantDoc ID 139635

Office 365 Deployment Options

Examining the plans, features, and monthly rates available for small and large businesses

by Tony Redmond

Companies that run Exchange Server 2003 or Exchange Server 2007 face an interesting choice as they consider their future messaging platforms. The traditional option is to continue with an on-premises deployment, upgrading the organization to Windows Server 2008 R2 and Exchange Server 2010 SP1. The alternative is to embrace the cloud and move some or all of the organization's mailboxes to a hosted platform. Microsoft has spent a lot of money (estimated at up to $2.5 billion) in building massive data centers around the world and in making server products such as Lync, SharePoint, and Exchange "cloud capable"—thereby forming the basis of its Office 365 offering, which was released in June 2011.

BPOS, the Predecessor to Office 365

Microsoft Business Productivity Online Standard Suite (BPOS) was released in November 2008 and was Microsoft's initial foray into the hosted market. Microsoft refers to Office 365 as the "technical evolution of BPOS." While BPOS is based on the 2007 versions of Exchange and Microsoft Office SharePoint Server (MOSS), Office 365 is based on the 2010 versions of these products.

BPOS includes Exchange Online, Office Communications Online, SharePoint Online, and Office Live Meeting, and it's available in standard (BPOS-S) and dedicated (BPOS-D) editions. The difference between the two is that BPOS-S uses a shared environment to host multiple companies, while a separate environment is created for each company that uses BPOS-D. Additionally, the dedicated versions of BPOS and Office 365 are intended to support businesses that have more than 5,000 users, which is the cutoff point that justifies the extra cost required to create a dedicated instance. The standard edition offers no room for a company to customize the services to meet its needs, as this is very much a utility service where you accept whatever the service provider delivers, just like electricity or water. There's more room to maneuver in the dedicated version, but you still have to accept that control rests in the hands of the service provider, and you can't customize Exchange or SharePoint as much as you can in an on-premises deployment.

Options to Buy Office 365

There is a wide range of options available to access Office 365. Microsoft breaks down the options into plans that are priced on a per-month basis. Note that the prices quoted here are US baseline prices, which you should verify with your local Microsoft office. The plans are for standard versions of Office 365. Replacement Office 365 offerings for the dedicated and federal versions of BPOS will follow in due course with their pricing subject to negotiation between Microsoft and customers.

Options for Smaller Businesses

Plan P is designed to support small-business users (any business with five or more users). This is an ultra-competitive market because it's where Microsoft goes head-to-head with Google Apps. Microsoft

charges $6 per month for a Plan P user, which includes the following:

- A 25GB Exchange 2010 mailbox (including an online archive) with access via Outlook or Outlook Web App (OWA)
- SharePoint 2010 team sites
- Office Web Apps
- A simple public website
- Lync online meetings and desktop sharing
- Multiparty IM and person-to-person calling
- Self-help, and what's charmingly referred to as "community support" (the opportunity to use your favorite search engine to look for an answer)

There's a lot of good functionality available here, and companies that run one or two Exchange 2003 servers today could see Plan P as an obvious path forward. However, these companies will have to invest in some extra network capacity if they want to move to Office 365 because their users will now depend on fast, dependable bandwidth to get their work done. Third-party resellers will also find opportunity with Plan P because they'll be able to sell services to help companies move mailboxes to Office 365 and then use some of the new features to set up team sites, create a website (if the customer doesn't already have one), train users to use Lync, and so on.

Options for Larger Businesses

Large companies are more complicated to plan for because of how many users (and types of users) need to be accommodated. Large companies often have users in multiple locations in different countries, have multiple operating units, and must meet numerous functionality requirements to satisfy their industry's regulations.

Factors that can complicate planning and deployment for large enterprises include the following:

- Some enterprises might need to create a hybrid situation where some users connect to servers running in the company's own datacenter and other users connect to Office 365. *Federation*, or the ability of servers running in either environment to share information such as free/busy data, is critical to providing a single unified service for users.
- Enterprises tend to use a wider range of devices.
- Some applications could have a dependency on Exchange or SharePoint. For example, Exchange often acts as an SMTP server that allows applications to send messages as part of their processing. Office 365 does not support public folders, which will deter companies that still use them to distribute and share information within their Exchange deployment.
- In an enterprise, actions that affect user productivity must be minimal. For example, restarting Outlook once after a mailbox is moved is acceptable, but components such as Autodiscover have to work flawlessly after they move to the cloud and must not generate calls to the Help desk because of connectivity problems.
- Greater importance is placed on quick and accurate 24 × 7 support that is provided by competent support professionals.

These factors create a complex operating environment for Office 365, and the planning for its deployment is often long and detailed. The intricacies of federation, synchronization, security, and monitoring must be worked through to create a situation where on-premises and cloud servers work together to deliver a seamless service.

Microsoft divides enterprise users into two camps: kiosk users and information workers. Plan K is designed for employees who don't spend much of their time using a PC. Factory workers are a good example—they may need email and access to team sites to participate in company communication, but they are largely passive consumers of communications rather than generators of new information. Users in this category tend to use a shared PC on a shop floor or some common area to infrequently update themselves about company information. Therefore, Plan K provides the following:

- 500MB mailboxes with access via OWA; alternatively, POP3 access is available, so some mobile clients are supported
- Access to SharePoint team sites, but no storage allocation
- Office Web Apps

Two variants are available. Plan K1 ($4 per month) is suitable for workers who need intermittent access to a company email system and only need to read Office documents. Plan K2 ($10 per month) includes Office Web Apps so that workers can edit documents.

Plan E is designed for information workers, who are the traditional consumers of Exchange and SharePoint. There are four variants (E1 through E4), which are priced from $10 per month to $27 per month. The top two variants (E3 and E4) include the right to install a copy of Office 2010 Professional Plus on a PC. All Plan E variants include the following:

- A 25GB mailbox with access from Outlook or OWA or mobile clients (ActiveSync or POP3/IMAP4).
- 500MB of SharePoint storage.
- Lync communications, including IM and presence.

Companies will probably spend time planning how to split their users across different combinations of K and E plans before they'll achieve the right balance of functionality and cost. This assumes that companies know their users and understand how they access and use existing on-premises services. But many companies don't understand who does what with Exchange, SharePoint, and other applications. It's easy to assign plans to obvious users—executives will all probably be assigned Plan E4 even if they don't use all of its features, while part-time staff might receive Plan E1 if all they need is access to email, a calendar, and IM. The users in the middle will provoke the discussions as planners seek the right combination.

Understanding the Real Cost of Deployment

It's easy to do the math and calculate a simple cost for Office 365. After all, you take the monthly cost of each plan and multiply it by the number of users that you assign to that plan and then total everything up. You might then tout all the savings that you can report to the CIO because you don't have to run expensive on-premises servers fully equipped with licenses and all the other costs that quickly mount up around a service such as email.

However, it's not quite as simple as replacing one big cost with a smaller

monthly cost, or as the accountants say, transferring a lot of capital expenditure to ongoing operational expenses. Other costs lurk under the surface of a cloud transition. Network costs are a good example. Most companies today have networks that are designed for internal communications and that reflect the links between internal data centers and their users in offices and other company locations. But when you move to the cloud, you transform your network needs to be outward-facing because the communications are now from clients working inside the company to servers located in remote data centers that are connected by the Internet. You have to be sure that your network infrastructure can cope with the changing demand and perform as well when accessing cloud services as it does when using internally located servers.

The costs of monitoring and reporting are also often overlooked. It's easy to monitor servers when they run in internal data centers and are completely under the control of the IT department. It's more difficult when you have no control over servers that are located somewhere in the cloud and that must be accessed by a resource that no one controls (the Internet). Big hosting providers such as Microsoft do a good job of providing dashboards to report service availability and known downtimes, but they measure availability only in their terms—often at the boundary of their data center—and not as a user would understand it ("Can I access my email?"). Therefore, it's important to measure and analyze performance so that you can be proactive if problems occur and so that you can hold the hosting provider accountable if it doesn't meet the service level agreement (SLA).

Transition to the cloud will also add to the cost of deployment. There are many tasks involved in the planning and execution of the move, including setting up Active Directory Federation Services (ADFS), enabling single sign-on, making sure that mailbox moves go smoothly and don't affect the operations of the on-premises servers, and ensuring that information such as free/busy data for mailboxes on both sides of the hybrid divide are available to all users.

Every company is different when it comes to calculating a cost profile. Some will continue to have extensive on-premises services, some will operate a hybrid model, and some will use the cloud for everything. It's vital that you do sufficient up-front planning so as to understand all the cost buckets that exist for cloud services. Then, you can run an apples-to-apples comparison and fully understand where savings can be made and where new costs will be incurred. Equipped with this information, you'll make a better decision about if (or when) the time is right for your company to embrace cloud services.

Using Office 365

Administrators are always judged by the quality of the service they deliver to users, so it's important to know just how good Office 365 is in the eyes of a user. I've been fortunate to be an Office 365 user for the last few months and have accessed my mailbox using Outlook 2010, OWA, and my iPhone. Office 365 was in beta when I used it, but even so, the experience was very good. The only glitches occurred when I used OWA on the Chrome browser (IE 7 or later, Firefox 3 or later, and Safari 4 or later are fully supported) and when I had to configure email access for my iPhone through IMAP instead of being able to use the Microsoft Exchange (ActiveSync) account type offered by the iPhone. This second glitch was ultimately resolved, as I was able to configure my iPhone to use ActiveSync to connect to an Office 365 domain a couple weeks after my first attempt. And, ultimately, these are small issues that are of little importance in the real world.

From a user perspective, using OWA or Outlook works exactly like it does when you're connected to an on-premises server. You need Outlook 2007 SP2 or a later version to connect to Office 365; Outlook 2011 for Mac is also supported. Client platforms include Windows 7, Windows Vista SP2, Windows XP SP3, Mac OS 10.5, and Mac OS 10.6. Upgrading to suitable versions of the desktop OS and Office applications could present some extra work for some companies, but the reality is that it's time to upgrade anyway if you're running older software.

As you can see from Figure 1, the only obvious difference that you'll see after you connect through OWA is the Office 365 logo in the upper-left corner and some additional options (such as the *Team Site* option) on the top menu bar. Figure 1 also shows that different themes are available and that Office 365 supports access to archive mailboxes. All the features supported by Exchange 2010 SP1, including MailTips and online archives, are available.

Administrative Access

Administrators use a web browser or Remote PowerShell to access Office 365 and perform

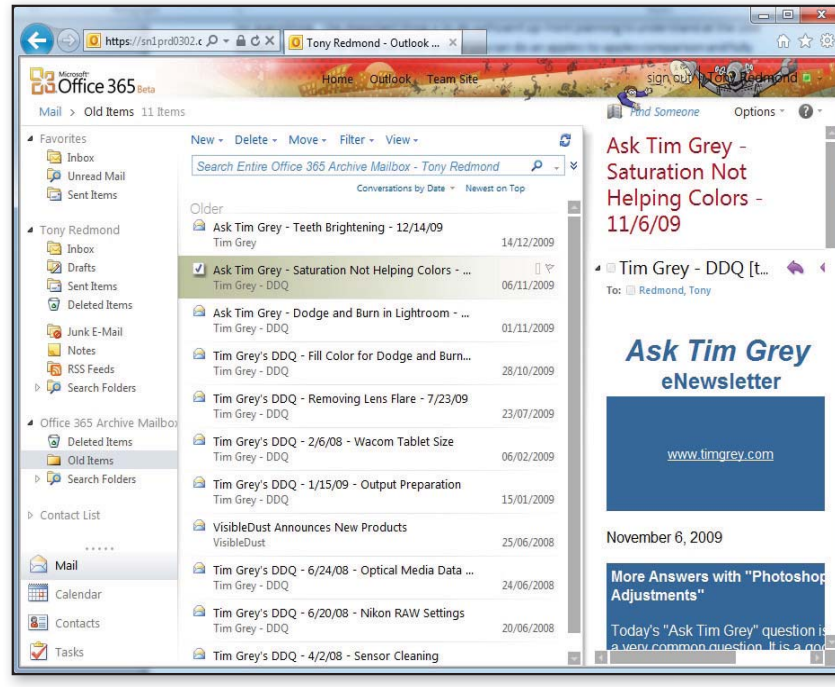


Figure 1: The OWA interface in Office 365

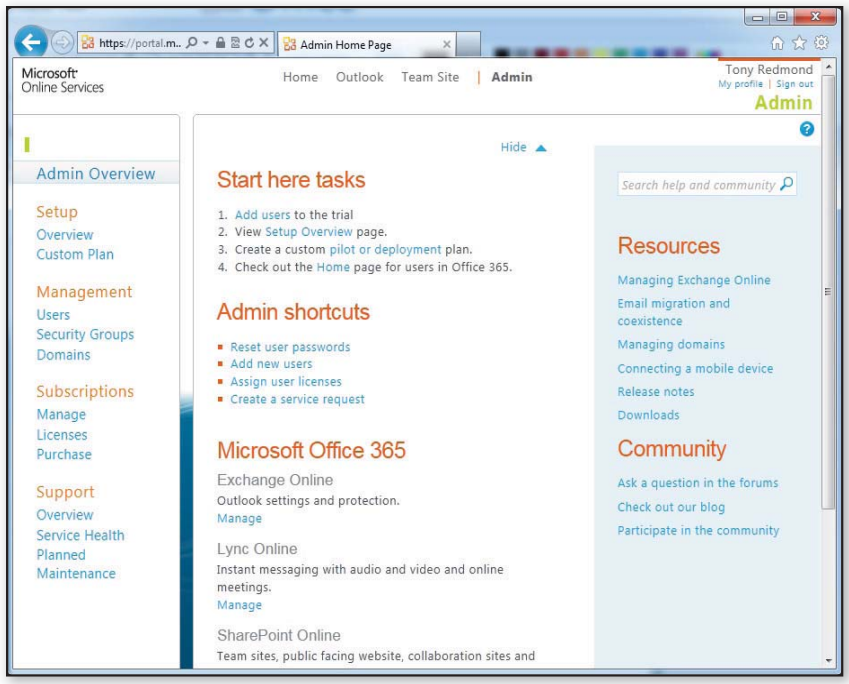


Figure 2: The Microsoft Online Services Admin Overview page

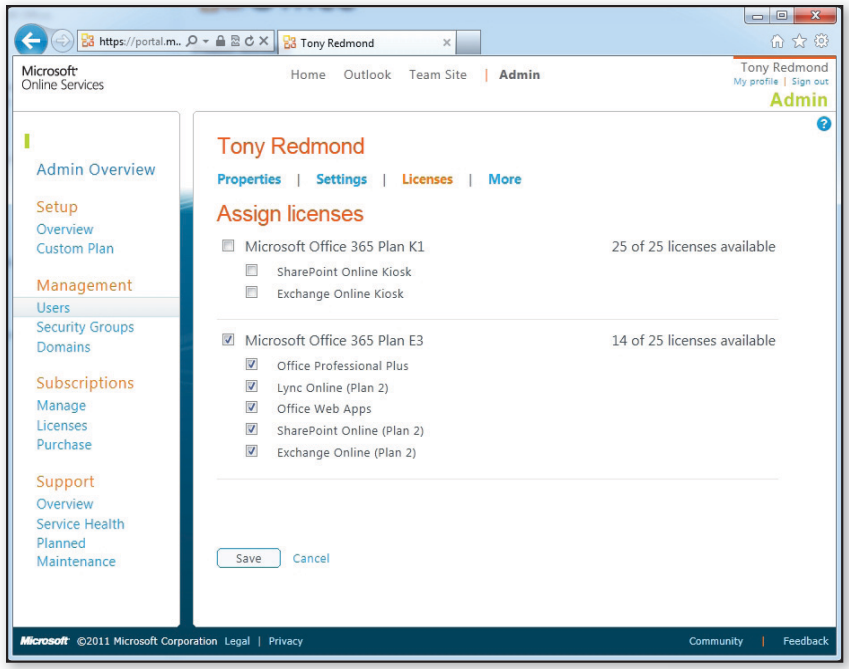


Figure 3: Reviewing license settings in Office 365

tasks such as creating new mailboxes. Tools such as Exchange Management Console (EMC) aren't used. Figure 2 shows the basic overview that an Office 365 administrator might see, and Figure 3 illustrates how a license is assigned to a user.

Exchange administrators in Office 365 use a modified version of Exchange Control Panel (ECP) and the Role Based Access Control (RBAC) feature introduced in Exchange 2010. In other words, ECP shows you the components that you're allowed to manage, as defined by the RBAC role groups to which your account belongs. Office 365 uses different RBAC groups than those defined for on-premises Exchange 2010, so you'll see groups with names such as "Tenant Admin" (all-powerful for managing users for a specific tenant) and "Help Desk Admin." Remote PowerShell is also available, so you can run PowerShell cmdlets and scripts (also controlled by RBAC) to perform administration through the shell. Figure 4 shows how an administrator can set the properties of a user's mailbox. This interface should be familiar to anyone who has seen the on-premises version of ECP.

Office 365 and Third-Party Companies

Third-party hosting providers have traditionally provided hosted Exchange. Microsoft provides a special hosting mode in Exchange 2010 SP1 for these partners, but hosting mode doesn't deliver the same functionality as Exchange running in Office 365. Microsoft has some unique features in Office 365, but it's important that Microsoft not lose sight of the fact that hosting partners have been faithful to the company for many years. Microsoft should support these partners' ability to, at times, compete with Office 365 on a reasonably level playing field.

Third-party software vendors have filled many gaps in Exchange functionality, including antivirus protection and reporting. When you use hosted applications, you're less likely to need third-party products, if only because you usually can't install software to work with servers that run in a hosted environment. This creates a real business problem for third-party software vendors. They can concentrate on a smaller set of on-premises customers, refocus their business entirely, or develop solutions that work with Office 365, understanding that they can't expect to have any administrative access to the servers. The most successful vendors will find some new functionality niche where they can deliver real value to an Office 365 deployment.

Companies that specialize in consulting or outsourcing Exchange won't be excited by the range of Office 365 plans as Office 365 eliminates much of their traditional market. Companies that choose Office 365 won't need an outsourcing partner, and those that choose the standardized deployment used by Office 365 won't need consultants to help them design and deploy Exchange or SharePoint. However, companies that require large and complex deployments of Office 365, especially those that involve hybrid configurations, will need to bring in a consultant if they don't have

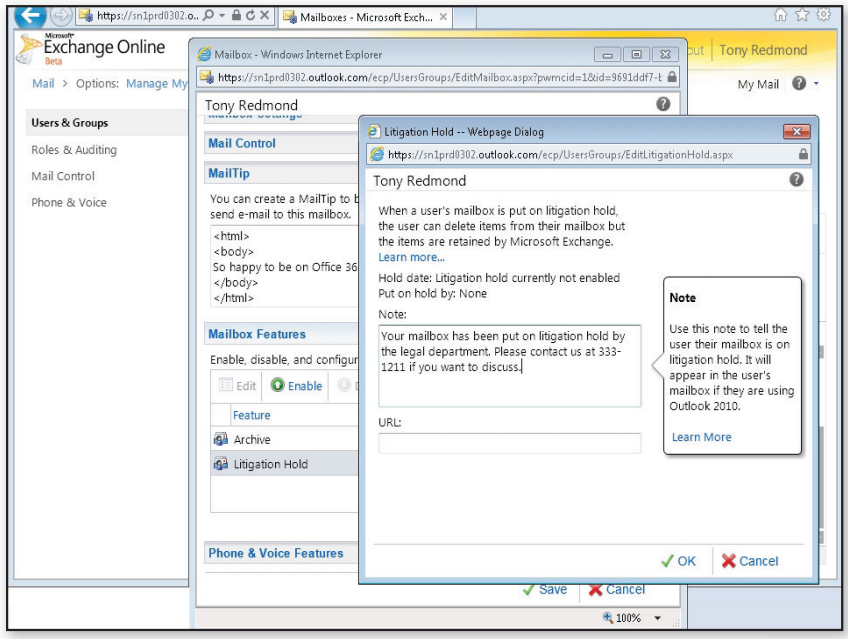


Figure 4: Modifying user mailbox settings

someone in-house who has the expertise and knowledge to manage it. As always, shifts in technology direction and focus force the consulting market to evolve.

On-Premises and Cloud Hosting: A Balancing Act

Serving two masters is never easy, and Microsoft must conduct a careful balancing act over the next few years to develop and grow its hosted market without alienating its on-premises customers. Nobody likes to be forced into a choice, and customers won't be pleased if they perceive that Microsoft is pouring all its resources into an effort to serve its Office 365 base, thereby neglecting its on-premises Exchange market.

Office 365 now has a huge influence over Microsoft Office applications, and that influence will only increase as Microsoft engineers work to improve their ability to offer hosted server applications, making them a viable alternative to traditional on-premises deployments. Office 365 already offers new opportunities—whether forging a hybrid approach or soaring fully into the cloud.

InstantDoc ID 135867

Tony Redmond
(12knocksinna@gmail.com) is a contributing editor for *Windows IT Pro* and author of *Microsoft Exchange Server 2010 Inside Out* (Microsoft Press). His blog is available at thoughtsofanidlemind.wordpress.com.

FEATURE

Introduction to Cluster Shared Volumes

Hyper-V architecture basics for improved storage

by John Savill

Microsoft Hyper-V was introduced in Windows Server 2008. This enterprise-ready virtualization solution provides true hypervisor-based virtualization that enables virtual machine (VM) performance that's equivalent to running on native hardware. Hyper-V uses failover clustering as the mechanism to create highly available Hyper-V environments. This feature enables the ability to move a VM from one node to another with minimal downtime through quick migration, which essentially saves the VM memory and state to disk, pauses the VM, dismounts the LUN on the current VM owner node, mounts the LUN on the target VM owner node, reads the memory and state information back into the VM on the target, and then starts the VM. This process is fairly fast but typically makes the VM unavailable for about 30 seconds (or longer, depending on configuration), which causes users to be disconnected.

One of biggest shortcomings of Server 2008's Hyper-V is its inability to move a VM between nodes in a failover cluster without any downtime. For Hyper-V to realistically compete against other virtualization solutions, it needed an overhaul in Server 2008 R2 for its VM migration technology. This revamp required two major changes. First, it was necessary that a VM's memory and state could be copied between nodes while the VM was still running. This change would avoid the long downtime associated with saving memory to disk and then reading from disk on the target machine. Hyper-V Server 2008 R2 introduced Live Migration to address this issue. Second, Hyper-V 2008 R2 removed the LUN dismount and mount operation, which was necessary to make the configuration and Virtual Hard Disk (VHD) available to the source and target nodes simultaneously. This article focuses on the second Hyper-V change in Server 2008 R2.

The Shared Nothing Problem

NTFS is a very monogamous file system. An NTFS volume can be accessed and used by only one OS instance at a time; it wasn't designed as a cluster file system. However, NTFS is also a very powerful file system: highly secure, industry tested, and with a huge support ecosystem that includes backup, defragmentation, and maintenance tools, as well as many services that rely on features of the file system.

A cluster consists of multiple nodes, each running an instance of Windows Server. But when NTFS volumes are used in a cluster, how is the integrity of NTFS maintained, and how are multiple concurrent mounts of an NTFS volume prevented? In a failover cluster, shared disks (i.e., disks that all the nodes in a cluster have a path to—which means they're typically LUNs on a SAN) are resources of the cluster. Like other resources in a failover cluster, these resources have only one owner at any one time. Therefore, multiple mounts of a LUN are blocked because only one node can own the resource. The resource owner mounts the LUN and can access the NTFS volumes stored in the LUN.

Consider Hyper-V using failover clusters—particularly VMs. This lack of sharing introduces several design considerations. Hyper-V uses disks to store not only the VHD for the VM but also for the various configuration and state files. If an NTFS volume can't be accessed by more than one node at a time, any VMs that share a LUN for storage of the VHD and configuration must run on the same node. Moving one VM on its own that shares a LUN for storage with another VM isn't possible; all the VMs sharing the LUN must move as a collective unit. This restriction means that in Server 2008, each VM must have its own LUN so that each VM can be moved independently of other VMs around the cluster, by dismounting the LUN and mounting on the new node. A limit of one VM per LUN means administrators must deal with a lot of LUNs, as well as a lot of potential wasted space, because each LUN is provisioned with a certain amount of space and room to grow.

In addition to extra management of multiple LUNs and the potential for a lot of wasted space, another problem with Hyper-V in Server 2008 is the act of dismounting the LUN from the current owning node and mounting on the target node when a VM needs to be moved. This dismount/mount operation takes a lot of time. The goal in Server 2008 R2 was to achieve a zero-downtime migration solution for VMs, with no visible end-user effects. The Hyper-V team implemented Live Migration to transfer memory and state information without stopping the VM. However, dismounting and mounting the LUN that contains the VHD requires a pause of the VHD, which results in downtime. To prevent the need to dismount and mount during moves and to avoid having one LUN per VM, as well as to save space, prevent administrative headaches, and—ultimately—save money, it's necessary to have a LUN that's accessible by all nodes in the cluster at once.

Cluster Shared Volumes

Although NTFS has a sharing issue, SANs themselves have no problem with multiple concurrent connections to a LUN, which means that the only changes necessary involve the file system or how it's accessed. One option is to create a whole new file system that's clusterable; however, this solution requires a lot of development and testing—plus, it negates all the support and trust in NTFS. Another solution is to fundamentally change NTFS and how it handles metadata updates; however, changing NTFS in this manner would be a Herculean task and would require numerous changes to the Windows OS, as well as changes to many applications and services that use NTFS—not to mention the additional testing required.

Microsoft's solution to the shared nothing problem was to make NTFS sharable without changing the file system at all—which seems like an obvious solution but is more difficult to implement than you might think. Server 2008 R2 achieves this goal with the addition of Cluster Shared Volumes.

NTFS has problems with concurrent access because of the way it handles metadata changes, which are changes that affect the actual file system structure, such as file size. Having multiple entities updating the metadata at the same time can lead to corruption. Cluster Shared Volumes solve this problem by nominating one of the nodes in the cluster as the owner for each Cluster Shared Volume (i.e., the coordinator). That owner node then performs all metadata updates to the volume, while the other nodes can perform direct I/O to the volume—which for virtualization loads is the majority of the access, such as reading and writing to a VHD. The owner node has the Cluster Shared Volume locally mounted and therefore has full access. Each Cluster Shared Volume disk has its own owning node, rather than having one node nominated to be the owning node for every Cluster Shared Volume disk in the cluster. Multiple nodes can be owners for different Cluster Shared Volumes. The owning node selection is dynamic in nature. If an owning node is shut down or fails, then another node automatically becomes the owning node for any Cluster Shared Volume disks on that node.

This separation of metadata activity and normal I/O is achieved through the introduction of the Cluster Shared Volume filter into the file system stack on each node in the cluster when the Cluster Shared Volume is enabled. When a non-owner node needs to make a change to metadata, such as a file extend operation on a dynamic VHD, then that metadata change, which is generally small in size, is captured by the Cluster Shared Volume filter and sent over the cluster network to the owning node, which performs the metadata update on behalf of the non-owning node. The network used for the Cluster Shared Volume communication between the owner and non-owner nodes is the same network used for the cluster health communication (i.e., the cluster network). The non-owning nodes can perform direct I/O to the LUNs because the Cluster Shared Volume filter actually creates a sector map for each Cluster Shared Volume disk that shows where the file data resides. This map is shared with all nodes in the cluster, giving them direct access to the correct sectors.

As Figure 1 shows, both nodes have connectivity to the storage. However, the LUNs are actually locally mounted on the owning node, which can perform both data and metadata actions, whereas the non-owning node can perform only direct I/O, such as reads and writes of blocks on disk.

An important point here is that Cluster Shared Volumes are a solution for Hyper-V VM workloads; as such, this solution has

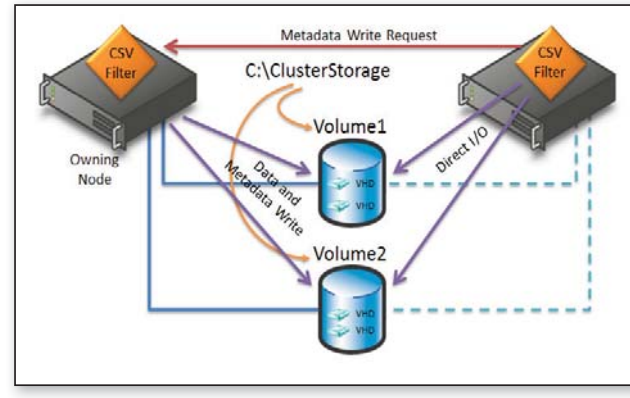


Figure 1: Cluster shared volume architecture

been optimized around the way in which VMs use storage. Cluster Shared Volumes shouldn't be used nor are they supported for anything other than storing Hyper-V VMs. When you enable Cluster Shared Volumes for a failover cluster through the Microsoft Management Console (MMC) Failover Cluster Management snap-in, you must accept the dialog box terms and restrictions that explain that the Cluster Shared Volume can be used only for files created by the Hyper-V role.

The Cluster Shared Volume filter provides an additional benefit to storage access within the failover cluster. Normally, the Cluster Shared Volume filter intercepts metadata activity and passes these requests to the owner node for action; however, the filter can also intercept all I/O made to a Cluster Shared Volume disk and pass over the cluster network to the owning node for execution. When this interception of all I/O is used, the Cluster Shared Volume disk is in redirected mode. It's important to understand why this ability is important.

You should eliminate single points of failure in any high-availability solution. Microsoft Multipath I/O (MPIO) is a great solution to allow multiple paths to storage, which eliminates a single point of failure for accessing storage. Problems can still occur, and many installations don't use MPIO—which is where redirected mode can be a life saver. If a node in a cluster loses the direct connectivity to a LUN hosting a Cluster Shared Volume disk (typically because of a problem connecting to the SAN hosting the LUN), then the access to the Cluster Shared Volume automatically switches to redirected mode until the node reestablishes direct connectivity to the LUN. In the meantime, all the I/O is sent over the cluster network to the owning node and executed, which lets the node that lost connectivity to the storage continue functioning with no interruption to the VMs, as Figure 2 shows. In redirected mode, a lot more traffic is sent over the cluster network. This consideration is important in selecting the specifications for the cluster network (e.g., 10Gb versus 1Gb). Only the node that lost connectivity to the LUN goes into redirected mode for the Cluster Shared Volume hosted on the LUN. Other nodes in the cluster that still have connectivity will continue to perform direct I/O and only send the metadata over the cluster network to the owning node.

Beyond connectivity failures, certain types of maintenance operations don't work well with multiple OS instances directly writing to blocks on disk. This is another reason for redirected mode—sometimes it's necessary to have only one node writing to a disk. Manually placing a Cluster Shared Volume disk in redirected mode accomplishes this. When you manually place a Cluster Shared Volume disk in redirected mode, all nodes in the cluster go into redirected mode for the specific Cluster Shared Volume disk. All I/O for the Cluster Shared Volume disk for all nodes is then sent over the cluster network to the owning node for that specific Cluster Shared Volume disk.

Cluster Shared Volume Requirements

Cluster Shared Volumes don't have any specific requirements regarding shared storage within a failover cluster. If the storage is available as shared storage within a cluster, it can be added to the Cluster Shared Volume namespace and made accessible to all nodes in the cluster concurrently. However, there are some network requirements when Cluster Shared Volumes are used, especially with Live Migration. When you use Cluster Shared Volumes, some storage actions take place related to metadata being sent over the network rather than directly to the storage. The network needs to be low latency to avoid introducing any lag in disk operations but typically doesn't need to be high bandwidth because of the minimal size of the metadata traffic under normal circumstances.

The cluster network has specific configuration requirements to support Cluster Shared Volume communication, in addition to some configuration on the nodes themselves. The cluster network should be a private network that only the network adapters that are used for the Cluster Shared Volume are connected to. The IPv6 protocol must be enabled, because Microsoft's development and testing was based on IPv6. IPv4 can be disabled on the cluster network adapter.

Because the Cluster Shared Volume communication between nodes occurs via Server Message Block (SMB), the *Client for Microsoft Networks* and *File and Printer Sharing for Microsoft Networks* services must be enabled on the network adapter that's used for the cluster network (as well as the Cluster Shared Volume). Disabling NetBIOS over TCP/IP on the network adapter is also recommended.

On the failover cluster nodes, ensure that the server and workstation services are running and that NTLM hasn't been disabled. Although failover clustering uses Kerberos exclusively for its normal operations, NTLM is required for the Cluster Shared Volume communication over the cluster network. NTLM is typically disabled through Group Policy; therefore, checking the Group Policy Resultant Set of Policy (RSoP) results will help confirm that NTLM isn't disabled. A great way to actually check SMB connectivity between nodes is to run the command

```
net use * <cluster network IP address
  of another node>\c$
```

on all the nodes.

Picking the Cluster Network

I discussed the cluster network for transporting Cluster Shared Volume traffic, which is typically just metadata but in redirected mode could be all the I/O for a

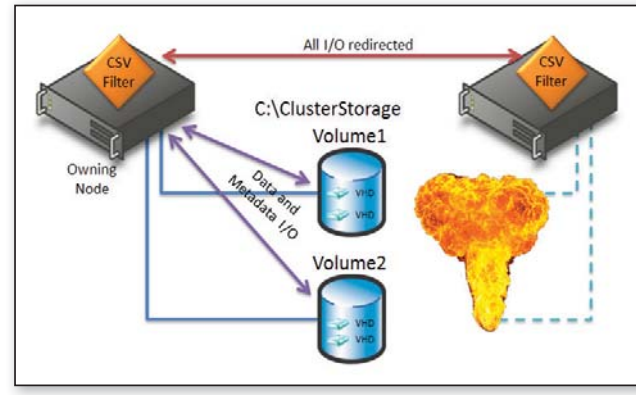


Figure 2: Redirection of I/O in the case of lost connectivity

Cluster Shared Volume disk. It's important to architect your networks to ensure optimal performance and availability.

With Server 2008 failover clusters, you don't usually have only a single network that the cluster can use for communication—which would constitute a single point of failure. Instead, the Network Fault Tolerant (NetFT) driver picks a network to use for the cluster communication, based on several attributes of the available networks.

For each network that's available in the cluster, the administrator can specify whether the network can be used for cluster communication, such as cluster health and Cluster Shared Volume traffic, and whether clients can connect through the network, as Figure 3 shows. These settings are used to calculate a metric for each network adapter. The metric assignment is such that a cluster-enabled network that isn't enabled for client communication, and therefore is used only for cluster communication, will have the lowest metric and therefore will more likely be used by NetFT. Given the critical role of NetFT with Cluster Shared Volumes, you need to ensure that your cluster has a dedicated network—only for cluster communication—that's connected to a gigabit or higher dedicated switch to prevent disruption to heartbeat communication and avoid false failovers.

To see all your networks, including which metric they've been assigned, you can use Server 2008 R2's new PowerShell Failover Clustering module, as follows:

```
PS C:\> Import-Module FailoverClusters
PS C: > Get-ClusterNetwork | ft Name,
  Metric, AutoMetric
Name                Metric   AutoMetric
----                ------   ----------
Client Network      1000     False
Cluster Network     100      False
iSCSI Network       10000    True
LM Network          110      False
```

The first line imports the Failover Clustering module; the next line lists the cluster networks, which are then formatted into a table.

Note in my example that AutoMetric is false for my Client, Cluster, and Live Migration networks. I set these metrics manually, to ensure that NetFT always uses the network I want for cluster communication and the Cluster Shared Volume.

To set a metric, you must first create an object pointer that points to the network. For example:

```
$netobj = Get-ClusterNetwork "Cluster
  Network"
```

Now that we have the object pointer, we can modify its Metric attribute as follows:

```
$netobj.Metric = <custom value, i.e.
  100>
```

You should be careful when using this method. Typically, if you set all other attributes correctly (e.g., which networks can be used by the cluster, which networks are exclusively for client communication), you don't need to manually change the metrics.

If you're using Live Migration in the cluster, Live Migration uses the network with the second lowest metric, by default. This prevents the Live Migration traffic from clashing with the cluster and the Cluster Shared Volume traffic. You can use the Failover Cluster Management snap-in to change which networks Live Migration can use for each VM, via the *Network for live migration* tab of each VM's properties.

Networks are an art unto themselves, with failover clusters that use Cluster Shared Volumes and Live Migration—and even more so when iSCSI is used. In this scenario, you'd typically see five network adapters, which might actually consist of multiple physical network adapters teamed together for resiliency and performance:

1. One network adapter for management of the Hyper-V host
2. At least one network adapter for virtual networks used by the VMs
3. One network adapter for cluster communication and the cluster shared volume
4. One network adapter for Live Migration traffic
5. One network adapter for iSCSI communication

For more information about network adapters, see the Microsoft TechNet article "Hyper-V: Live Migration Network Configuration Guide" at technet.microsoft.com/en-us/library/ff428137(WS.10).aspx. This article discusses all the network adapters you might have, including how to best separate the various types of traffic. I also provide information about cluster network configurations at www.savilltech.com/videos/CSVDeepDive/CSVDeepDive.wmv.

Using Cluster Shared Volumes

Using a Cluster Shared Volume is easy. After you add available disk storage to the Cluster Shared Volume, the volumes on the disk are exposed as folders under the \%systemdrive%\ClusterStorage folder, which by default are named Volume1, Volume2, and so on. On a node with C as the system drive, the first Cluster Shared Volume would be accessible as C:\ClusterStorage\Volume1, the second Cluster Shared Volume as C:\ClusterStorage\Volume2, and so on, as Figure 4 shows.

Every node in the failover cluster has exactly the same ClusterStorage namespace, all with the same volumes and content. You can rename VolumeX, but you can't rename the ClusterStorage folder. Note that each Cluster Shared Volume doesn't need a drive letter; therefore, there are no restrictions based on available drive letters and no more management through a globally unique identifier (GUID). Your VMs and VHDs are placed in a volume under \ClusterStorage

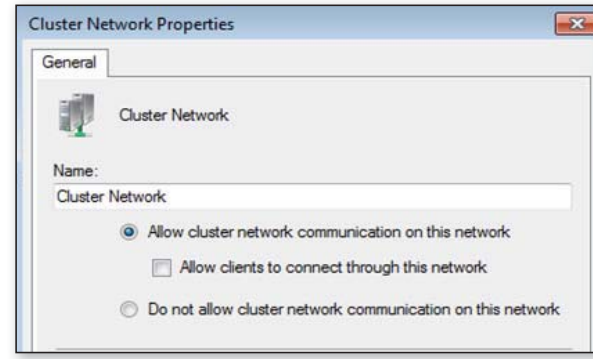


Figure 3: Setting cluster network properties

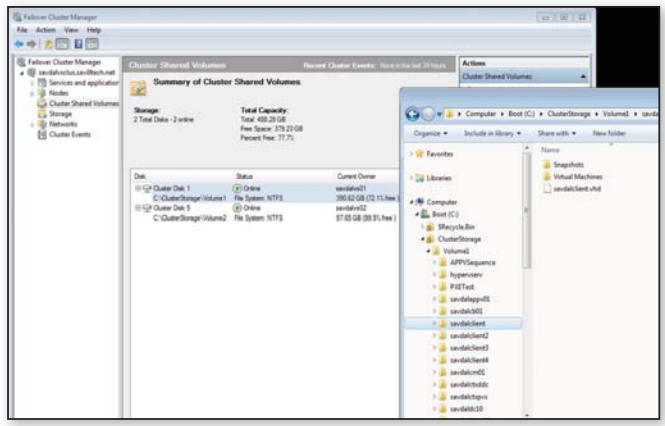


Figure 4: Cluster Shared Volume folder structure

and used as usual. Nothing special needs to be done—although this doesn't mean there are no considerations to take into account.

Server 2008 requires you to put one VM on each LUN, to enable maximum flexibility in VM placement and migration. With Cluster Shared Volumes, all the VMs and VHDs can sit on a single Cluster Shared Volume–enabled LUN. But just because you *can* put all VHDs on one LUN doesn't mean you *should*. Consider the typical rules for placing application data or databases, log files, and the OS on separate disks. If all these VHDs are on the same Cluster Shared Volume, you lose a lot of the benefit of different disks providing protection. To provide better protection, you might instead want to consider separate Cluster Shared Volumes, with one designated to store OS VHDs, one to store log VHDs, and one for application data or database storage.

Performance is also critical. You need to consider your VMs' I/O operations per second (IOPS) requirement. Putting numerous VMs on a single LUN might help cut down on management and wasted space; however, you need to understand the capabilities of the LUN to ensure it meets the combined IOPS requirements of all the VMs on the LUN.

Maintaining Cluster Shared Volumes

As I mentioned earlier, having every node able to directly access the blocks on Cluster Shared Volumes is great for flexible architecture, availability, and functionality but does introduce some complications when you consider volume maintenance. Many utilities expect exclusive access to a volume and its blocks during operation. Imagine running a disk defragmentation on an owning node, while meanwhile another node writes to a block on the disk that the defrag operation just moved—not good! Consider Microsoft Volume Shadow Copy Service (VSS) backups, Chkdsk, and so on—none of these operations would work if multiple nodes could write to blocks on the disk while the backup or utility was trying to run.

This is the situation in which placing a Cluster Shared Volume disk in redirected mode is important. However, the good news is that you don't have to worry about this as long as you use utilities and backup software that support Cluster Shared Volumes.

Actions such as the Inbox defragmentation utility and Chkdsk should be performed through the Repair-ClusterSharedVolume PowerShell cmdlet, which automatically places the Cluster Shared Volume in redirected mode, performs the tasks, and then takes the Cluster Shared Volume out of redirected mode to resume normal operations.

Backup vendors also have access to a special API call: PrepareVolume ForSnapshotSet(). This call automatically places the Cluster Shared Volume in redirected mode and releases it after the backup is complete. If you're performing a hardware-based VSS snapshot, the redirected mode should be required for only a few seconds. A software-based VSS snapshot, however, might keep the Cluster Shared Volume in redirected mode for quite some time while the backup completes.

Multisite Considerations With Cluster Shared Volumes

Server 2008 introduced widespread support for multisite clusters spanning multiple subnets. However, the cluster network that Cluster Shared Volumes use must be a single subnet network. This means that although all the other networks used by the cluster can cross the subnet, you must use some kind of stretched Virtual LAN (VLAN) for the cluster network.

For the actual storage, various hardware and software vendors support the replication of Cluster Shared Volumes and ensure that the integrity of the Cluster Shared Volumes is maintained. You only need to be sure that your VM replication solution supports Cluster Shared Volumes.

The question often comes up regarding why DFS Replication (DFSR) can't be used to replace Cluster Shared Volume content between sites. DFSR is a great solution to replicate files; however, it works by replicating the changes to a file when the file closes. With VMs, files remain open all the time until the VM is stopped—which isn't useful for most needs.

Easier Than You Might Think

Cluster Shared Volumes give Hyper-V environments the flexibility necessary for VM placement and the capability to enable storage optimization. Cluster Shared Volumes don't change the underlying file system but instead open up a volume's availability to all nodes in the cluster simultaneously. Therefore, the learning curve for using Cluster Shared Volumes is fairly small because an environment's processes and tools typically don't need to change to allow these storage management changes.

Although we typically think of Cluster Shared Volumes and Live Migration as working together for zero downtime VM migration, the two technologies are separate. Cluster Shared Volumes can be used even if Live Migration isn't used. Using Cluster Shared Volumes alone still lets organizations simplify storage management and optimize storage while gaining VM placement flexibility.

InstantDoc ID 139786

John Savill
(john@savilltech.com) is a Windows technical specialist, an 11-time MVP, and an MCITP: Enterprise Administrator for Windows Server 2008. He's a senior contributing editor for *Windows IT Pro*, and his latest book is The *Complete Guide to Windows Server 2008* (Addison-Wesley).

Mastering Exchange 2010's Exchange Control Panel

The ECP provides a variety of functions for different users

by Brian Desmond

One of the new feature areas in Microsoft Exchange Server 2010 is the Exchange Control Panel. The ECP is a web-based configuration interface for Exchange that has the ability to be many things to different groups of people. For end users, when you click Options in Outlook Web App (OWA), the UI for managing account settings is part of the ECP. For delegated administrators (e.g., branch office administrators, service desk technicians), the ECP is a friendly interface for managing the properties of accounts and groups. For the Exchange administrator, the ECP provides an alternative interface to some settings and the only graphical interface for others. Finally, for administrators of hosted organizations (e.g., Microsoft Office 365 tenants), the ECP is the primary option for managing Exchange features specific to the organization.

End-User Functionality

Most of the functionality offered by the ECP to end users when they click Options in OWA is nothing new to OWA or Exchange. The usual functions, which are also available in Outlook—such as configuring calendar options, an email signature, or an Out of Office message—are all present. In addition to these options, there are several new functions that are available to end users only through the ECP. These functions include the ability to manage the data in your Global Address List (GAL) entry, as well as the ability to manage distribution lists and security groups for which the user is an owner. Other useful functions specific to the ECP include access to delivery reports (message tracking to Exchange administrators), the ability to manage mobile devices and text messaging (SMS), and access to information such as IMAP and POP server settings.

Self-service management of address book data for end users has been a requirement of small and large organizations for more than a decade. Until Exchange 2010, numerous third parties provided products directed at this capability. The only other option was a typically shaky home-grown solution. Exchange 2010's solution isn't likely to be as flexible as most third-party solutions, but it fills the needs of the vast majority of the market.

Figure 1 shows the self-service GAL editor on the front page of the end-user Options screen in the ECP. The fields available in the editor are fixed, but they cover the important bases, such as name, phone numbers, address, and so on. As you can see in Figure 1, I can edit my phone numbers; however, my name is read-only, as evidenced by the gray text boxes. As an administrator, you can use Role Based Access Control (RBAC) to configure whether users can edit specific fields on an individual basis. Because of the flexibility of RBAC, you don't need to apply the same policy to all users; for example, you might want to limit employees to editing only their mobile phone numbers but allow contractors to edit their work phone numbers and their mobile phone numbers.

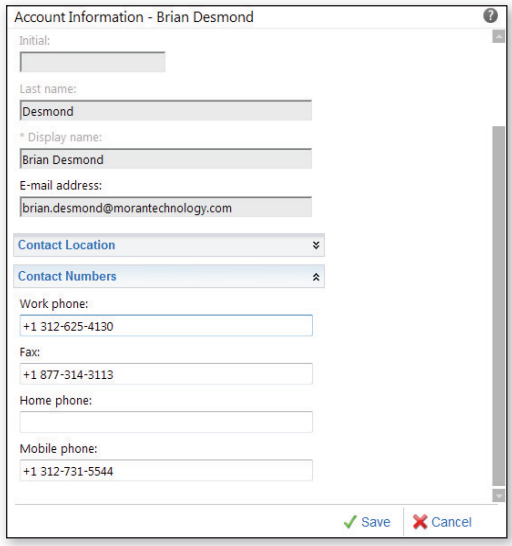


Figure 1: Self-service GAL entry management

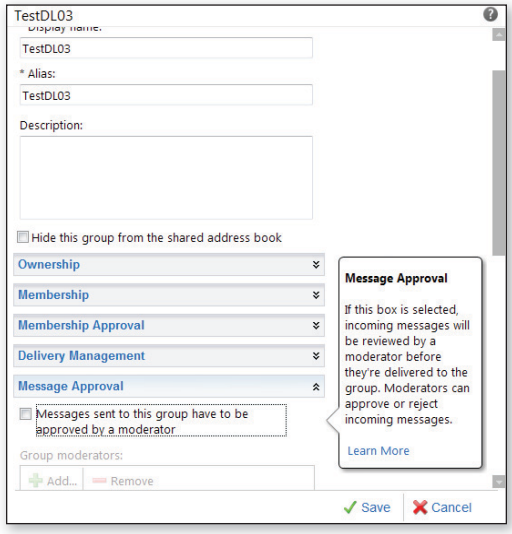


Figure 2: Managing group settings in the ECP

Another market that's been ripe for add-on products since the early days of Exchange is self-service management of distribution lists (DLs). Outlook has always offered users the capability to add and remove members from a DL if they have appropriate access; however, this ability often doesn't provide nearly enough functionality. Many organizations need the capability to delegate the creation and deletion of DLs, as well as provide the ability for end users to join and leave groups without administrator assistance.

Exchange 2010 introduced all this functionality natively, accessible through the ECP. Users can create and delete DLs, as well as manage all the properties of the lists they own. In addition to managing lists, end users can join and leave distribution groups that are listed in the GAL. Much like the self-service GAL management functionality, all the functionality revolving around the management of groups is controlled through RBAC. Administrators can easily allow users to manage groups they own but not allow them to create new groups, for example. Figure 2 shows some of the properties available for management by group owners. Exchange 2010 SP1 adds the ability for users to manage security groups as well as DLs, making the group management functionality in the ECP significantly more compelling for many organizations.

Another notable end-user feature in the ECP is what Microsoft calls *delivery reports*. Exchange 2010 provides a summarized end-user friendly interface into traditional message tracking logs, which lets users review the status of messages they've sent. To speed up access to the logs, Exchange now stores indexes of them alongside the logs, which allows for quick lookups. Delivery report information is available through several entry points.

Outlook 2010 users can select Delivery Reports on the Outlook 2010 Backstage area and Outlook will launch a web browser and browse directly to the ECP. OWA users can view delivery report information in two places. To check the status of a specific sent message, users can right-click a message in their Sent Items folder and select Delivery Report. A search interface is also available in the Options area under Organize E-Mail, as Figure 3 shows. Users with administrative privileges will receive additional detailed information when accessing delivery reports.

Delegated Administration Features

The ECP includes several useful features that can be delegated to junior administrators or technicians so they can complete requests without involving an administrator. Common examples include modifying user or group properties; modifying mailbox settings, such as Inbox rules or Out of Office messages; and performing message tracking at the organization level.

Technicians who've been delegated sufficient access can manage numerous user mailbox properties beyond those delegated to an end user. A common example is the ability to add and remove additional email addresses (proxies) from a mailbox. Although only existing mailboxes can be managed, groups and contacts can be created and deleted through the ECP.

Service desk analysts often receive calls from end users requesting assistance in modifying mailbox settings or performing simple tasks such as setting an Out of Office message. With sufficient access, analysts can open the same Options screen that an end user would see and modify settings on the user's behalf. Exchange limits the analyst to modifying the settings that the end user would normally have access to so that organization-level permissions aren't bypassed. This functionality can be delegated without granting access to the actual contents of user mailboxes.

With the Exchange 2010 Enterprise CAL, you can use multi-mailbox search functionality to perform e-discovery across the organization or a group of mailboxes. Prior to Exchange 2010, this task often required expensive third-party tools or

Figure 3: End-user delivery reports search

OCTOBER 31-NOVEMBER 3, 2011

LAS VEGAS, NV ■ MANDALAY BAY RESORT & CASINO

WINCONNECTIONS conference and expo

WINDOWS CONNECTIONS
Microsoft® Exchange CONNECTIONS
UNIFIED COMMUNICATIONS CONNECTIONS
SharePoint CONNECTIONS
SQL Server CONNECTIONS

THE CONVERSATION BEGINS **HERE**

QUESTIONS ANSWERED • STRATEGY DEFINED • RELATIONSHIPS BUILT

KEYNOTES

QUENTIN CLARK
MICROSOFT
CORPORATE VICE PRESIDENT, DATABASE SYSTEMS GROUP, MICROSOFT SQL SERVER

STEVE FOX
MICROSOFT
DIRECTOR, DEVELOPER AND PLATFORM EVANGELISM FOR SHAREPOINT

MARK MINASI
MINASI RESEARCH AND DEVELOPMENT

TONY REDMOND
TONY REDMOND AND ASSOCIATES

JEFFREY SNOVER
MICROSOFT
DISTINGUISHED ENGINEER AND LEAD ARCHITECT FOR WINDOWS SERVER DIVISION

KEVIN ALLISON
MICROSOFT
GENERAL MANAGER, EXCHANGE

EARLY BIRD DISCOUNT!

Register by September 19th and book a minimum of three nights at Mandalay Bay and you'll receive a $100 Mandalay Bay Gift Certificate and save $100 off conference registration!

REGISTER TODAY!

www.WinConnections.com
800.438.6720 • 203.400.6121

Microsoft® SSWUG.ORG Your Database Answers Are Here SQL ServerCentral.com SQL Server magazine Windows IT Pro TECH Conferences Inc. PENTON MEDIA

The Next Generation of Technology Is Coming. Are You Ready?

Find Out About These Game-Changing Technologies at the Fall 2011 Connections Conferences!

SCHEDULE AT A GLANCE

SUNDAY, OCTOBER 30, 2011	
7:30 am	Registration Opens
9:00am - 4:00 pm	Pre-conference Workshops
MONDAY, OCTOBER 31, 2011	
7:30 am	Registration Opens
9:00am - 4:00 pm	Pre-conference Workshops
6:00pm	Keynotes
TUESDAY, NOVEMBER 1, 2011	
7:00 am - 5:00 pm	Registration
7:00 am - 8:00 am	Continental Breakfast
8:00 am - 9:15 am	Keynote
9:15 am - 10:15 am	Expo Hall Open
10:15 am - 12:30 pm	Conference Sessions
12:30 pm - 2:00 pm	Lunch
2:00 pm - 4:30 pm	Conference Sessions
4:30 pm - 5:30 pm	Keynotes
5:30 pm - 7:00 pm	Expo Hall Reception
7:00 pm - 8:00 pm	Vendor Sessions
8:00 pm	Ad-hoc Community Events
WEDNESDAY, NOVEMBER 2, 2011	
7:00 am - 5:00 pm	Conference Registration
7:00 am - 8:00 am	Continental Breakfast
8:00 am - 9:00 am	Keynote
10:00 am - 12:45 pm	Conference Sessions
12:45 pm - 2:15 pm	Lunch
2:15 pm - 5:30 pm	Conference Sessions
5:30 pm - 7:00 pm	T-shirt and Prize Giveaway
7:00 pm	Open Spaces at DevConnections, INETA User Group Session, Q&A Panels
THURSDAY, NOVEMBER 3, 2011	
7:00 am - 8:00 am	Continental Breakfast
8:00 am - 1:00 pm	Conference Sessions
10:30 am - 2:30 pm	Expo Hall
1:00 pm - 2:30 pm	Lunch
2:15 pm	Cruise Raffle
2:30 pm - 3:30 pm	Conference Sessions
4:00 pm - 4:30 pm	Closing Session & Prize Drawing
FRIDAY, NOVEMBER 4, 2011	
9:00 am - 4:00 pm	Post-conference Workshops

Get ready to LEARN as we deliver 250+ in-depth sessions...get ready to NETWORK with 150+ Microsoft and industry experts...get ready to STRATEGIZE with thousands of your peers from around the world! And when the day ends, get ready to PARTY because you are in LAS VEGAS!

Events at WinConnections

We're adding more and more to WinConnections each year. Check out a few of the things you can do after the technical sessions end for the day.

- Open Spaces is sponsored by User Community. This is an open forum to discuss various subjects of concern to developers, DBAs and IT pros. Lead a session or listen in.
- INETA User Groups meeting.
- Q & A Panels. Come prepared to change your thinking and get differing opinions on the future of technology.
- Women in Technology Luncheon on Wednesday, November 2, 2011.

WINDOWS CONNECTIONS
Microsoft Exchange CONNECTIONS
UNIFIED COMMUNICATIONS CONNECTIONS
SQL Server CONNECTIONS
SharePoint CONNECTIONS

BONUS TRACKS: > OFFICE 365 > EVALUATING / MIGRATING TO THE CLOUD

CO-LOCATED WITH

Microsoft Silverlight CONNECTIONS
Microsoft ASP.net CONNECTIONS
HTML5 CONNECTIONS
Microsoft Visual Studio CONNECTIONS
Windows Azure CONNECTIONS

You can attend any of the co-located sessions for no additional charge.

CONFERENCE AND EXPO INCLUDES

Windows, Exchange and Unified Communications Connections registration includes a one-year (12 issues) print subscription to ***Windows IT Pro*** magazine for Windows, Exchange and Unified Communications conference attendees only. Current subscribers will have an additional 12-months added to their subscription. Subscriptions outside of the United States will be served in digital; $12.50 of the funds will be allocated toward a subscription to ***Windows IT Pro*** ($49.95 value).

Your conference registration includes:

- Three Lunches
- Reception
- Proceedings CD
- Three Continental Breakfasts
- Conference T-Shirt and Bag
- Evening Sessions *and much more!*

Join Us!

at Open Spaces sponsored by User Community Wednesday night at 7pm!

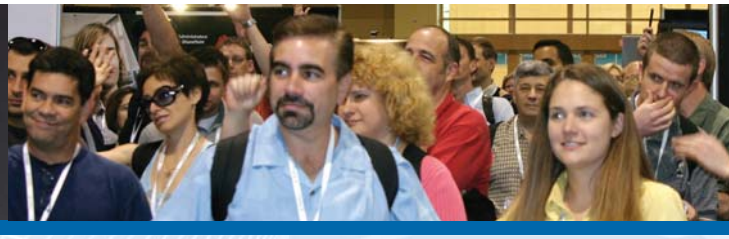
USER COMMUNITY
join in
MicrosoftUserCommunity
@usercommunity

Cruise Giveaway!

Enter the contest to

WIN A 1 WEEK CARIBBEAN CRUISE FOR TWO!

You must be present in the Expo Hall at the time of the drawing to win.



MICROSOFT SESSIONS

Deploying Windows Server to the Physical and the Virtual Worlds

Windows Server 2008 R2 SP1 Features: Dynamic Memory & RemoteFX

Get Ready for Windows 8 by Migrating/Upgrading to Windows 7

Windows 7: Cool Tips, Tricks and Features We Can Use Right Now!

Leveraging Windows Intune to get You Ready for Windows 8

Windows Server and Client Management on the Cheap: Using Free and Built-in Tools to Manage Your Infrastructure

The Virtual Windows Desktop – An Overview of App-V and Med-V

Hardening Windows 7: Additional Security Tips

More sessions will be added. Check the website closer to the show date for more details.

KEYNOTE SESSIONS

KENOTE: Changing Datacenters, Changing IT

Jeffrey Snover

Technology and economics are fundamentally changing the nature of datacenters which has a direct effect on IT. Some will prosper, others will not. This keynote session puts aside the plethora of pundit prognostications to concentrate on critical core changes and identify IT Pro initiatives needed to survive and prosper in the new world.

KEYNOTE: How Windows Can Win: What Microsoft Needs in the Next Windows

Mark Minasi

Windows 7 and Server 2008 R2 are out and have been for nearly two years, but much of the world still uses "Windows 5.5" – XP and Server 2003, and yet rumor has it that we'll see another version of Windows in 2012. Given buyers' current choice to adopt new versions of Windows slowly or not at all, is a new Windows a good idea or a bad one? And, more important, if a new Windows COULD revivify the market, what would it need to include? In this wide-ranging keynote session, veteran Windows watcher, 25-year columnist and bestselling author Mark Minasi presents his take on what the next Windows needs more of AND what that version of Windows needs LESS of. Come for the laughs, but stay for the insights!

SECURITY

WIN10: Conducting a Forensic Computer Investigation for IT Staff

Mike Danseglio

Computer crime has been on the rise for decades. There are many situations where an incident occurs that doesn't break the law but is still cause for concern, such as corporate policy violations, information mishandling, or internal system compromise. Many companies are forming their own internal investigative units to address these situations. In this session, Mike Danseglio - CISSP, a world-renowned security expert who has conducted hundreds of these investigations for both private organizations and law enforcement, will explain what kinds of investigations can be handled internally, when and how to engage law enforcement, how to best prepare for incidents, and the best practices to use. Mike will also focus on building your computer investigation toolkit including the tools you should have and the structured process of how you should use them.

WIN13: Portable Data Security on Laptops, USB Drives, and More

Mike Danseglio

From the CEO who loses her USB drive at Starbucks to the human resources manager who has his laptop stolen on vacation, data compromise is commonplace today. It shows up in the news daily. But the stories you don't see are the ones where data is lost but protected so well that the only value of the lost device is its pawn shop price. So how do you protect data like that? It's a combination of people, process, and technology. This session focuses on technologies that provide strong data encryption without being expensive or a nightmare to administer and use. There are simple to implement and largely idiot-proof technologies that you should be implementing and enforcing today. Mike Danseglio - CISSP, a world-renowned security expert, will show you the strengths and weaknesses of technologies including Bitlocker, Bitlocker-to-Go, Encrypting File System, BIOS passwords, Syskey, hardware-based data encryption, and many more that you have probably never seen. Focus is placed on the relative security (cryptographic strength) of each solution but, unlike many presentations, purchase cost, cost of ownership, and usability are also explored. You will see live demonstrations of tools you probably already have at hand. At the end of this session you'll know the best data protection solution for your unique situation.

WINDOWS SESSIONS

WIN01: Microsoft System Center Orchestrator 101: Your Secret IT Pro Automation Buddy, Engine, and Secret Weapon

Jeremy Moskowitz

The original name of this product was the super-cool name "Opalis Robot" so you know it's gotta do some kick-butt stuff. What does it do? It's your code-free automation engine to push the hundreds of buttons from system to system, move data from system to system and automate the heck out of your hectic world. When an alert or condition happens, you want to know about it, of course, but you also want the problem to "just magically go away." If you can dream of the "automatically fix it" scenario, System Center Orchestrator (SCO) is there to be your invisible (and automatic) arms and fingers. In this session, you'll learn about the moving parts of SCO as well as some key scenarios where you can use this tool right away.

WIN02: Total Workstation Lockdown: Your Action Plan

Jeremy Moskowitz

Total workstation lockdown isn't for every machine in your organization but some machines require it. It's usually those "public walk up" machines that we need to manage a little bit differently. These kinds of machines are in the cafeterias, the lobby and the library. Microsoft has a variety of technologies you can choose (and mix and match) to make your workstations as locked down as they need to be. In this session, Group Policy MVP Jeremy Moskowitz will demonstrate a myriad of ways to make your public desktops more secure. If your team is already using Group Policy, come learn about common GP Scenarios, the GP Preferences, and how to efficiently use loopback processing. Learn about some non-Microsoft tools to help enhance your PC control.

WIN03: Microsoft Windows Intune: Manage Your Desktops from the Cloud (and Like It!)

Jeremy Moskowitz

Taking advantage of the cloud doesn't have to mean "moving your server farm and PC universe over to someone else's data center." It could mean "sit on the beach and manage a dozen PCs remote-

ly." That's Windows Intune. It's Microsoft's "cloud service" to enable administrators of small, medium and large organizations to set desktop policies using the Interwebs. From patch management, to inventory to configuring firewall policies – Windows Intune is quickly growing to deliver "Group Policy-like" functionality over the Internet. Want to see what's inside? See you at this session!

WIN05: Rebuilding SteadyState: Tips to Create More Robust Windows... and It Won't Cost You a Cent!

Mark Minasi

As any operating system – Windows included – gets more complex, it also gets more fragile. Where once simple OSes like DOS could be fixed in moments by replacing a file or running SYS C:, Windows is so complex that the most oft-used repair tool for many is "wipe and re-image," and that's a shame, as it burns up both IT pro and end-user time and productivity. Wouldn't it be great to add the virtual machine notion of "snapshots" to physical Windows 7/R2 systems, like Microsoft's now-defunct SteadyState did for XP? Or how about being able to take a working system that no longer boots and restore its ability to boot in under three minutes? And while we're at it, why not add a smaller "maintenance version" of Windows to your Windows 7, Server 2008 and 2008R2 systems, an on-disk "emergency platform" for examining, diagnosing and repairing troubled systems? Two years ago, veteran Windows techie and writer Mark Minasi set out to build something like SteadyState, using some of Windows 7 and R2's new storage and boot technologies. Along the way to creating his free "RollWinBack!" tool, he had to develop several new Windows repair and installation techniques, and in this session you'll learn how they work and how they can make your systems somewhat more robust. In this session, you'll first learn how to take a system whose boot record and/or boot configuration database (BCD) has been corrupted and rebuild those structures by hand in just about a dozen commands. Then you'll see how to build a copy of WinPE, Microsoft's free "repair and deploy" OS, to your computer either as a retrofit or as an as-installed option to your PC's hard disk – once you've done that, you'll be able to tackle a whole range of "the system can't boot" problems without having to search around for a boot disk. Once we've mastered that, we'll move along to seeing how to build a physical Windows system with real-life snapshots through use of the boot-from-VHD facility and differencing VHDs.

ACTIVE DIRECTORY

WIN08: 7 Steps to Read-Only Domain Controllers in Your AD

Brian Desmond

Are you looking to increase your Active Directory security? In this session we'll look at seven easy steps to adding Read-Only Domain Controllers (RODCs) to your network and upgrading your Active Directory's security. We'll make decisions about protecting passwords, respond to an RODC incident, and of course best practices for placing and running RODCs. In this session, Active Directory expert Brian Desmond will unravel the RODC and make sure you know exactly where it fits on your network and the steps you need to take to deploy RODCs and manage them for the long run.

GENERAL

WMS10: The Tail Is Wagging the Dog: The Consumerization of IT and What it Means for YOU

Romi Mahajan

The world of the IT professional is a bit like a large gymnasium. You have the bodybuilders strutting around with Big Iron on the one hand and the aesthetes doing tai chi and yoga on the other. In the middle you have a bunch of normal people doing normal things – working hard and hoping for good results. In the gym, it's clear who is king – Big Iron is. Interestingly that was true in IT as well until recently when finesse, innovation, and democratization won over and the stalwarts of the older era died off in one generation.

The change in hierarchy has gone even further of late. In 2011, the yoga-loving, latte-sipping aesthete has won out both in the gymnasium and in IT. In the former, the point is clear. In the latter, the metaphor has to be understood in the context of the recent domination of consumer-led IT over enterprise IT. The industry's mindshare has been colonized by consumer devices and applications (which isn't to say that spending has shifted to the same extent.) What was considered "nice to have" has become "have to have" and enterprise has the choice of adapting to consumer-driven technologies or presiding over the complete disruption of how today's Information Workers conduct their business and their lives.

The tail is indeed wagging the dog. Bark as it might, the dog better get used to it.

VIRTUALIZATION SESSIONS

WIN14: Server Virtualization and High Availability Options for Your Company

Alan Sugano

Virtualization and High Availability sounds like an oxymoron. Of course with multiple virtual server guests running on a single host, a hardware failure can have a significant impact on business operations. But when virtual server images are stored on a Storage Area Network (SAN) you can achieve high levels of server consolidation, with high availability. This session will review your options for virtualization and high availability, and discuss the pros and cons of each solution. This session will cover High Availability solutions for both stand alone hosts and clusters.

WIN15: How to Incorporate Virtualization into Your Company's Disaster Recovery Plan

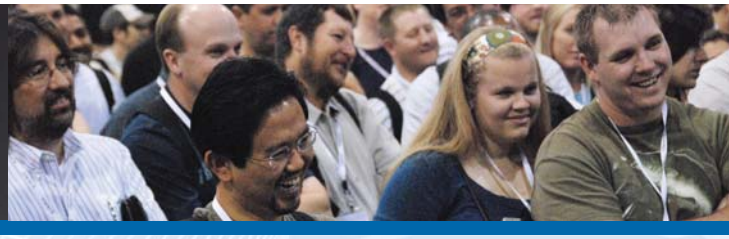
Alan Sugano

A comprehensive Disaster Recovery Plan is something that every company should have and hopefully will never have to use. Having a plan in place that provided a road map to recovery was adequate in the past, but recent emphasis has been placed on the speed of the recovery. Sarbanes-Oxley (SOX) compliance companies must disclose their business continuity plans and the company's exposure to a prolonged outage and how it affects financial reporting. Virtualization can significantly reduce the recovery time for a major disaster, by providing a warm or hot remote recovery site and accelerate workstation and server setup.

WIN16: Selecting a SAN for Your Virtualization Cluster

Alan Sugano

So you know you need High Availability for your Virtualization project, but which SAN is the best fit for your company? This session will focus on SAN selection for a VMware Cluster, however, many of the deciding factors are relevant when creating a Hyper-V cluster as well. iSCSI, Fibre Channel, 10GigEthernet, NFS, Fibre Channel over Ethernet (FCoE) which one is the best fit for your needs? What about remote SAN replication, Disaster Recovery, Tiered Storage, LUN Sizing, RAID Configuration, SAS, SATA, Disk Deduplication, Performance, Management and other factors? If you speak to a SAN vendor their SAN is the best and everyone else's SAN is a piece of junk. We'll demystify the various selection factors to help you get the best solution for your company.



PANELS AND Q&A SESSIONS

PANEL01: Gamification: Making IT Fun, Engaging, and Important

Romi Mahajan

Let's gameize IT!

Every large economic opportunity comes accompanied with a core theme, a mantra around which people can rally. These themes then generate a vernacular that takes on a life of its own and serves to fire the engines of inspiration in generations of entrepreneurs, investors, and practitioners. Recent examples of such themes are: Web 2.0, cloud computing, location-based services, marketing services, software-as-service, e-commerce – and scores of others. There's a new theme that might eclipse all of these – gameization. It has the potential to be a fundamental trend because it cuts across businesses and because it is as much about process as it is about products. Ignore it at your own peril.

So what is this concept and why is it so big? And how do you apply it to your job as an IT professional?

To understand this, come listen to this panel of experts and industry luminaries as they discuss and deliberate.

TIPS & TRICKS

WIN04: Windows Power Tools Treasury: Best of the Power Tools

Mark Minasi

Smart Windows administrators know that the only way to get the job done is to find the right tools, but so many interesting-looking tools are so poorly-documented that no one's got the time to figure out how to make them useful. That's why Windows techie Mark Minasi has taken the time every month from November 1997 onward to research and explain those tools in his "This Old Resource Kit" and "Windows Power Tools" columns, featured monthly in ***Windows IT Pro*** magazine. What's that you say? You've not had time to check out all thirteen year's worth? No problem: Mark's here to offer a fast-paced, entertaining look at some of the best power tools he's uncovered over the years. Come explore the power of sc.exe, the Swiss Army Knife of service tools, and its oddly excitable nature. See how you can unleash robocopy on your file transfer tasks, and still manage to get home in time for dinner. Learn some useful "stupid Netmon tricks," discover how to smoke out Active Directory replication issues with repadmin, even if your company doesn't allow smoking on the premises. And that's just the start – don't miss a chance to get a quick look AND some useful, accurate examples of a couple of dozen of the most powerful of Windows power tools!

TROUBLESHOOTING

WIN07: Hardcore Windows Troubleshooting

Brian Desmond

Ever wondered what to do when Windows gives you a blue screen? Cursing Microsoft is a common starting point, but, chances are it's a problem you can solve and it's not even Microsoft's fault. Have you ever had your manager breathing down your neck when the print server crashed? What about when the file server started moving really slow and hung? In this demo heavy 400-level session, we'll walk through how to troubleshoot and solve all of these common problems. Things we'll look at include analyzing several blue screen memory dumps and system memory, looking at just how Windows interacts with print drivers (you'll be surprised), and a walk through several packet captures. You'll walk away with an understanding of what causes the problem as well as the tools and methodologies to tackle them without calling support.

WIN09: The Laws of Network Troubleshooting

Mark Minasi

Network software and hardware comes and goes, protocols grow and change, and what we do with networks expands all of the time, but one thing doesn't change: how often we use the words "network" and "not work" in the same sentence. One day we'll just plug it all in and it'll just work, but for now, "to network is to troubleshoot." In this session, veteran networking consultant, teacher and writer Mark Minasi shares the twelve immutable laws of troubleshooting any network problem. Zen archers are reputed to be able to hit a target blindfolded; with this session, you can become a Zen network troubleshooter and fix network problems with both hands tied behind your back!

NETWORKING

WIN06: Networks for AD Pros

Brian Desmond

Been trying to act like you know what your network guys are talking about in a meeting? Ever wondered which combination of site links, bridges, costs, schedules, and connection objects is the right one? Come learn just how all those pieces work and when you have to worry about them, because it's never a network problem (right?) If you've got even a few sites on your network, chances are you'll need to work with a networking team to map your replication to the network. Chances are even greater the network folks will drop some terms you've never heard in that meeting. Plan to leave this session with an understanding of those terms and a solid understanding of how all the pieces fit together, and practical examples of how to apply them to real-world sample networks.

WIRELESS

WIN11: Deploying Windows Wireless Networks

Dr. Avril Salter

Windows 7 supports a growing number of wireless networks including Wi-Fi, Bluetooth and mobile broadband. These radio technologies are very distinct and require different considerations when configuring client access. While many of these are configurable through Group Policy settings in an Active Directory setting, you need to know which settings to change and what values will give you the desired configuration. This is a rare opportunity to hear from one of the few people that can explain all aspects of wireless in a way that makes sense to computer professionals. In this session, Dr. Avril Salter will enable you to compare and contrast radio technologies supported by Windows, describe the key technical aspects of each network that you need to understand to configure computers correctly, and determine the right Windows configuration for appropriate yet secure data access.

WIN12: Wireless Sniffing for IT Pros, Not Hackers

Dr. Avril Salter

The IT pro has a great variety of network monitoring tools and techniques available today. But many believe these are the tools of evildoers or spies. This session dispels the myth by showing how to use tools like Wireshark and NetStumbler to capture, analyze, and troubleshoot common wireless problems during everyday operations. Dr. Avril Salter has been sniffing wireless networks and showing folks how to identify common traffic issues for years. In this session she will show you a number of examples of wireless problems including rogue access points and misconfigured Windows settings that broadcast sensitive data as well as more expected issues like nefarious intruders and audio and video streams overloading network capacity.

CHECK WEB SITE AS WE CONTINUE TO ADD MORE SESSIONS, SPEAKERS AND MAKE UPDATES WWW.WINCONNECTIONS.COM


MICROSOFT SESSIONS

Recent Engineering Developments in Exchange 2010 – SP2

Load Balancing Connections (CAS, Load Balancers)

Interoperability with Exchange Online – Keeping Things Running as You Migrate

Migration to Exchange Online

Virtualizing Exchange with Database Availability Group

Complex Database Availability Group Designs

More sessions will be added. Check the website closer to the show date for more details.

KEYNOTE SESSIONS

KENOTE: Changing Datacenters, Changing IT

Jeffrey Snover

Technology and economics are fundamentally changing the nature of datacenters which has a direct effect on IT. Some will prosper, others will not. This keynote session puts aside the plethora of pundit prognostications to concentrate on critical core changes and identify IT pro initiatives needed to survive and prosper in the new world.

KEYNOTE: Why Microsoft's Head Is in the Cloud and what this Means to You

Tony Redmond

The Microsoft Exchange Development group takes care of both on-premises (Exchange 2010) and cloud (Office 365) versions of Exchange. Given all the hype around the announcement of Office 365, there's some reasonable concern that Microsoft might be focused on developing its cloud software to the detriment of the traditional on-premises version. In this session, Tony will explore why Microsoft has a focus on the cloud and what this means for future versions of Exchange, how the role of an administrator might change in the future, and what positive and productive steps you can take to prepare for a world when organizations can choose between on-premises, cloud, or hybrid deployments.

EXCHANGE SESSIONS

EXC01: To Backup or Not Backup - That Is the Question

Michael B. Smith

This session will focus on Exchange Native Data Protection. We will discuss the prerequisites for native data protection and the enablers in Exchange 2010 that make a backup-less environment feasible. For those that choose to backup, we will also discuss the implementation of Volume Shadow Services with Exchange 2010. Throughout the presentation we will incorporate experiences gained and look at issues received through support for these technologies.

EXC02: Exchange 2010 Mailbox Role High Availability - What's Under the Hood....

Tim McMichael

In this session we'll take a peek under the hood of Exchange 2010 Mailbox Role High Availability. We'll start by taking a look at the core Windows operating system components that make Exchange high availability possible and how they are leveraged. We'll then move onto Exchange 2010 installations and high availability concepts including the replication service, log shipping, and self-healing databases. Throughout the presentation we will incorporate experiences gained and look at issues received through support for these technologies.

EXC03: Exchange 2010 Mailbox Role Site Resiliency - Understanding Datacenter Activation Coordination

Tim McMichael

In this session we'll take a look at the implementation, management, and use of an Exchange 2010 Mailbox Role Site Resilient solution. We will look at the concept of Datacenter Activation Coordination and explain how this is utilized in this implementation. We will also review activation steps for multiple implementations. Throughout the session we will incorporate experiences gained and look at issues received through support for these technologies.

EXC04: Exchange 2010 Designing for Unified Messaging

Anthony Vitnell

The Exchange Unified Messaging role has introduced a completely new concept for Exchange Administrators. This role introduces new design criteria such as telephony integration, dial plans, and linguistic issues that must be addressed. In this deep-dive session we will build on real customer experiences and walk through the Unified Messaging design requirements, explain what happens when the UM server receives a call, and look at deployment architectures. In addition we will discuss the limitations of the Unified Messaging role and provide strategies to work around these limitations. At the conclusion of this session you will have the knowledge required to design the Unified Messaging role for your organization. An understanding of basic Telephony and Voice mail features and protocols is recommended for this session.

EXC05: Lync and Exchange Integration

Byron Spurlock

Microsoft Exchange Server 2010 Unified Messaging (UM) and Lync Server 2010 can be deployed together to provide voice messaging, instant messaging (IM), enhanced user presence, audio/video conferencing, and an integrated email and messaging experience for users in your organization. This session presents common integration scenarios for Exchange Server 2010 Unified Messaging and Lync Server 2010. We will break down the steps for deploying an integrated Exchange Server 2010–Lync Server 2010 Enterprise Voice solution. In addition, we will take a look at Lync Server 2010 instant messaging (IM) integration with Outlook Web App (OWA).

EXC06: Outlook Web App Customization in Exchange Server 2010 (Service Pack 1)

William Lefkovics

This session includes an overview of Outlook Web Application architecture, themes and web parts. We'll have a review of what is in the Exchange 2010 SP1 Outlook Web App Customization SDK and will conclude the session with some examples and demo of OWA customization.

EXC07: Exchange Virtualized or Exchange Physical – Where Do I Put those Bits?

Michael B. Smith

In this 300-level discussion, we will discuss the positives and the negatives associated with hosting your Exchange organization on virtual servers versus continuing with the traditional method of having your Exchange organization hosted on physical servers. In this technology deep dive, you will learn about various mechanisms available for providing high availability and fault tolerance on both virtual and physical infrastructures, and the reasons why moving to virtualization may be the "best thing ever" for your company or why it may be a horrible mistake. Targeted at technical decision makers and advisors, this session will provide

the most value to individuals who have a good understanding of the server and administrative requirements for their Exchange infrastructure and of their organization's needs for high-availability and fault tolerant services.

EXC08: SSL Certificates and Exchange – The (Next) Final Word

Michael B. Smith

Multiple-name SSL certificates (often called UCC or SAN certificates) became recommended (or required from some perspectives) in Exchange Server beginning with Exchange 2007. As an administrator might expect there are lots of opinions about how best to use these certificates, wizards to help configure them (both built into some versions of Exchange as well as from various vendors), and discussions as to whether the multiple-names are actually necessary and which roles of Exchange are best served with third-party or with self-signed certificates. In this session, targeted at implementers and upgrade administrators, we will discuss the current best practices for the creation and use of SSL certificates with Exchange, including the various roles; such as Edge, Hub, and Client Access.

EXC09: Economics of Cloud Sourcing and what that Means to Your IT Team

Jim McBee

Is your company considering moving an application you know and love off into the cloud? Though low cost of hosted business solutions are making the news recently, outsourcing applications to external providers is not new. As IT professionals, our obligation is not only to provide top-notch service to our end users but we also have to be fiscally responsible. This responsibility includes ensuring that services that are outsourced will meet your organization's requirements. This session will cover the economic value of outsourcing applications such as email to the cloud, discuss how to calculate the current cost of your email system, and cover factors to consider when your company is considering outsourcing.

EXC10: Don't Fear the Exchange Management Shell

Jim McBee

The Exchange Management Shell is one of the most powerful features of Exchange Server 2010 yet many administrators are intimiated by the shell and avoid using it. This session will get you started towards a happy life using the EMS to make yourself more productive. Topics include using the Exchange Management Console to learn the EMS, understanding objects, how the remote shell works, pipelining, simple scripting, and leveraging help from the shell prompt. Examples and demos in this session will include common administrative tasks. Exchange administrators that are intimidated by using the EMS should attend this session.

EXC11: My Exchange Server Is on a Fault Line (Establishing an Exchange 2010 Disaster Recovery Site)

Jim McBee

This session describes a number of best practices from organizations that have deployed Exchange 2010 Database Availability Groups (DAGs) across multiple sites to enhance their high availability capabilities and enable immediate restoration of service if disaster strikes the primary datacenter. Establishing a disaster recovery site for Exchange 2010 is more than adding an additional Exchange server and a few mouse clicks. Through in-depth discussion of practical notes from real-life deployments, attendees will learn about disaster recovery site prerequisites, common disaster recovery scenarios, and design issues to take into consideration when deploying a disaster recovery site. This session will also include detailed coverage of the steps necessary to switch over to the disaster recovery site and how to switch back. Exchange administrators planning to extend DAGs across multiple datacenters to provide disaster recovery capabilities should attend. A basic knowledge of Exchange 2010 and Windows Failover clustering is recommended. Exchange administrators that are planning to stretch DAGs across multiple sites will benefit from attending this session.

EXC12: In-depth Message Tracking Using the Tracking Log

Siegfried Jagott

This session will start off with an explanation of all the components of the Hub Transport role required for message routing. It will take this knowledge to the next level by matching the hub transport component's picture to the Queue Viewer as well as the Tracking Log Explorer. Understand what is happening under the hood when Exchange routes messages and how advanced message routing troubleshooting takes place. It's not hard to understand, but most people are just not practicing their skills in this important area of Exchange troubleshooting. You will understand how powerful the tracking log is, get to know the Poison Queue or the Pickup Directory and understand the implications of Accepted Domains on routing. You will also see some demonstrations about the techniques I will teach for troubleshooting using the Tracking Log Explorer as well as other tools.

EXC13: Rich Coexistence of Office 365 and Exchange 2010

Siegfried Jagott

Learn how to take advantage of Office 365 together with Exchange 2010 from a practical experience of a multi-national company. Understand the differences between simple and rich-coexistence with Exchange Online, and be able to plan and configure this for your own company easily. Make sure you make the right decision how to route messages when working in an on-premises and online coexistence. And finally, understand the implications of Forefront Online Protection for Exchange and what you should consider before implementing it. This session will also show you how to monitor the rich-coexistence to make sure it works as expected.

EXC17: Defend Your Lync Edge Server from DoS attacks, Brute-Force Password Attacks and Account Lockouts

Rui Maximo

This session covers how to protect valid user accounts from being attacked by providing an in-depth understanding of the authentication protocols used in Lync Server. Attend this session to get a free copy of the security filter for Lync Server to protect your Edge Servers from these sorts of Internet attacks.

UNIFIED COMMUNICATIONS

EXC14: Lync Server 2010 - Integration with the Cisco Telephony Platform

Anthony Vitnell

Achieving Unified Communications with Office Communications Server 2007 R2 and Cisco Unified Communications Manager produces countless integration scenarios that each provide different capabilities and benefits. Achieving telephony integration with Cisco Unified CallManager is a complex task, dependent on the versions implemented and additional Cisco / 3rd party software is often required. We will walk you through what level of integration can be achieved for each version of Cisco Unified CallManager, discuss the configuration requirements, and creative strategies to remove some of the limitations with older versions. This session will provide you with the information to determine the appropriate solution for your organization, and successfully integrate Lync Server 2010 with your Cisco Telephony environment. A basic understanding of Cisco Telephony components is highly recommended for this session.

EXC15: Lync Deployment Notes from the Field
Byron Spurlock

This session discusses lessons learned from field deployments of Lync Server 2010 with all workloads as IM/Presence, Conferencing, Voice Integration. We will cover real-world experiences in upgrading from OCS to Lync and cover strategies in preparing for a successful deployment as well as common pitfalls and traps to avoid in the process.

EXC16: I'm Not a PBX Guy. How do I Design and Deploy Lync Enterprise Voice?
Anthony Vitnell

For most Lync administrators, voice design and deployment topics are like a foreign language. In this session we will break down the voice components of Lync such as Dial Plans, Codecs, PBX integration/interop from a Microsoft administrators point of view. This session will provide you with the knowledge of the traditional voice world that you need to know to successfully design and deploy the Enterprise Voice features of Lync Server 2010. Using best practices and reference architectures from the field we will walk through a number of deployment and integration scenarios with leading PBX manufacturers such as Cisco, Avaya and Nortel to arm you with the information you need for a successful deployment. Attendees to this session do not need to be telephony experts, however, at the conclusion of this session you will have the information you need to talk like one.

EXC18: Configure Direct SIP with Lync Server and Skype Using Asterisk
Rui Maximo

Wish you could send an IM to an offline user so that they would immediately see it when they come online? Extend the reach of your Lync users to communicate with users on the Skype network. Join this session to see how to configure Asterisk as a gateway so Lync users can call Skype users. Come to this session for an early Christmas gift. You'll get a free copy of OMS for OCS 2007 R2 or Lync Server, and understand how easy it is to build UCMA applications.

PANELS AND Q&A SESSIONS

PANEL01: Gamification: Making IT Fun, Engaging, and Important
Romi Mahajan

Let's gameize IT!

Every large economic opportunity comes accompanied with a core theme, a mantra around which people can rally. These themes then generate a vernacular that takes on a life of its own and serves to fire the engines of inspiration in generations of entrepreneurs, investors, and practitioners. Recent examples of such themes are: Web 2.0, cloud computing, location-based services, marketing services, software-as-service, e-commerce – and scores of others. There's a new theme that might eclipse all of these - gameization. It has the potential to be a fundamental trend because it cuts across businesses and because it is as much about process as it is about products. Ignore it at your own peril.

So what is this concept and why is it so big? And how do you apply it to your job as an IT professional? To understand this, come listen to this panel of experts and industry luminaries as they discuss and deliberate.

OFFICE 365

EXC19: Lync Server 2010 Cloud
Byron Spurlock

Lync Online is Microsoft's cloud communications service and a key component of Microsoft Office 365. Come to this session to understand which Lync capabilities will be available in the cloud. The session covers IM, conferencing and voice in the cloud, as well as a comprehensive overview of hybrid cloud and on-premises deployment options for Lync and Office 365.

EXCHANGE AND SHAREPOINT

EXC20: SharePoint Online and The Cloud. Forecasting Today and Tomorrow
Randy Williams

The Cloud. SharePoint Online. Office 365. No doubt you have been inundated with marketing on Microsoft's cloud vision. Certainly the promised benefits of 99.9% uptime, safeguarded data, and a near maintenance-free environment saving time and money are compelling. However, technical issues such as authentication, migration, integration with legacy systems, and lack of server access may paint a cloudy picture. In this no-nonsense session, we'll look at Microsoft's current hosted SharePoint offering and give you the straight, unbiased story. Join us and you'll also get live demonstrations and the latest forecast on what you can expect in the future.

EXC21: Integrating SharePoint with Exchange: The What's, Why's and How's
Randy Williams

Are you looking for better synergy between your Exchange and SharePoint environments? Join us as we examine the primary integration points between these two products to be sure you are leveraging each to their fullest. We'll start by looking at how Outlook integrates with SharePoint, specifically when working with calendars, tasks, contacts and document libraries. We'll then see how using SharePoint's incoming email feature lets you send emails and attachments and have them filed inside lists and document libraries. Next is how SharePoint can index your current public folders to be sure this content can be found from within SharePoint's enterprise search engine. Lastly, we'll summarize migration options if you're looking to move public folders into SharePoint. Only a basic understanding of SharePoint is needed for this session.

Women in Technology Networking Luncheon

HOSTED BY


SUZANNA MORAN

Join us Wednesday, November 2

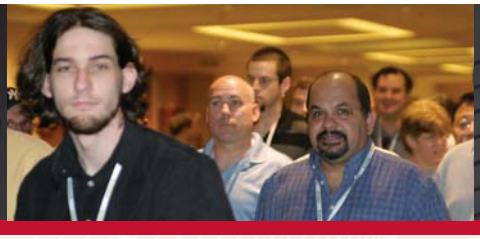

MICHELE LEROUX BUSTAMANTE

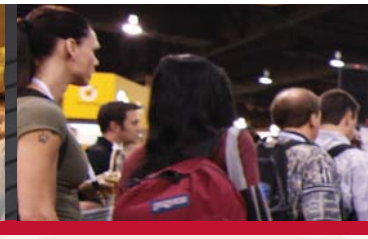

KATHLEEN DOLLARD


JULIE LERMAN


STACIA MISNER


KIMBERLY L. TRIPP





MICROSOFT SESSIONS

A lot of sessions for Microsoft SQL Server "Denali" are under wraps, but Microsoft will also be covering:

Enterprise Database Administration and Deployment

Database and Application Development

BI Platform Architecture, Development and Administration

SQL Azure

Check the website as we get closer to the show date for the Microsoft session titles and abstracts.

PERFORMANCE

SQL312: Building a BI Performance Monitoring Solution

Stacia Misner

Users expect business intelligence solutions to quickly deliver answers to their questions. When queries start slowing down, how do you determine the root cause of the problem? Is it the report server, the cube, the query, or server resource contention? Come to this session to learn how to use performance counters, report execution log data, and trace files to troubleshoot performance problems. You'll also learn how to set up a monitoring solution to capture data for benchmarking purposes before problems arise and for diagnostic purposes when queries start slowing down. You'll also learn how to interpret the performance monitoring data so that you can take the necessary steps to resolve performance problems in your BI solution.

SQL313: Filtered Indexes and Filtered Statistics: The Good, the Bad and the Ugly

Kimberly L. Tripp

SQL Server 2008 introduced a new type of index/statistic that has some unbelieveable power. However, it also has some troubles. In this session I'll show you why you will want to upgrade to 2008 (if you're not already there) and leverage these amazing filters. And, I'll also show you where they're a bit problematic with regard to updates and parameterization.

SQL315: How StackOverflow Scales with SQL Server

Brent Ozar

The most popular tech Q&A site in the world serves over 5 million web pages per day off a single SQL Server 2008 R2 instance. They're passionate about performance, and they'll share the scalability lessons they learned along the way. This session is aimed at production DBAs who manage SQL Servers that need to go faster and SQL programmers who don't understand why their database won't deliver queries quicker. You'll learn the basic infrastructure behind StackOverflow.com, the decisions made along the way while building the infrastructure, and how to tell when you need to make infrastructure and coding changes in order to scale.

SQL207: Precarious? Nefarious? Strategies that Work for Nonclustered Indexes!

Kimberly L. Tripp

Nonclustered indexes are the key to a server's overall health and performance but how do you create them? Do you trust the Database Tuning Advisor or the Missing Index DMVs? What do they tell you? And, why isn't SQL Server using a nonclustered index on a column that you have in the WHERE clause? Why does SQL Server choose one index (or one strategy) over another? How does all of this come together and how can you make the best of it? I'll start with a list of base table best practices but quickly move into "the tipping point" and the pitfalls of the tools. Finally, I'll end with demos that show how to best decide what types of indexes to create along with index consolitation best practices.

SQL405: Query Tuning Mastery: The Art and Science of Manhandling Parallelism

Adam Machanic

As a database developer, your job boils down to one word: performance. And in today's multi-core-driven world, query performance is very much determined by how well you're taking advantage of the processing power at your disposal. Are your big queries using every available clock tick, or are they lagging behind? And if your queries are already going parallel, can they be rewritten for even greater speed? In this session you will learn how to take full advantage of parallelism from a developer's point of view. After a quick terminology review and technology refresher the session will go deep, covering T-SQL patterns that allow certain queries to scale almost linearly across your multi-core CPUs. Alas, not all T-SQL queries can go parallel, so you will also learn to watch for those things that can restrict the query optimizer's decisions. Along the way you'll learn to manipulate costs and row goals, challenge generally accepted tuning practices, and take complete control of your parallel queries.

SQL401: Query Tuning Tips – Part I

Itzik Ben-Gan

This session is Part I of a two-part series. Given a SQL Server querying problem there's much that you can do to enable a good performing solution. Tuning involves arranging an optimal physical environment, e.g., by creating supporting indexes, as well as writing the query in a way that it would get an optimal execution plan. Many factors can affect the efficiency of the solution including the availability of indexes, data distribution and density, and others. In different scenarios, a different solution could be the most efficient for the same querying problem. Query tuning could be considered an art. This session will provide various tips to do efficient query tuning and demonstrate those through specific tuning examples. Among the query tuning tips that will be covered in this part (as time permits) are: Performance of Scalar Functions, Indexing Expressions, Descending Indexes, Top N Per Group Queries, TOP vs. MIN/MAX, Search Arguments, MAX/MIN Aggregates against Partitioned Tables, and others.

SQL404: Query Tuning Tips – Part II

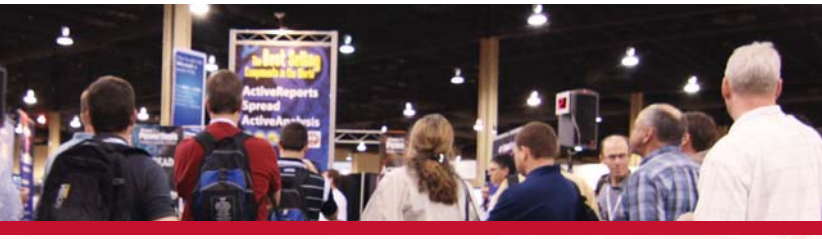
Itzik Ben-Gan

This session is Part II of a two-part series covering query tuning tips, though attending Part I is not a prerequisite. The two parts provide independent tips. In Part II you will learn about common query tuning challenges in SQL Server and how to address those efficiently. As time permits, this session will cover topics such as: Bushy Plans, Dynamic Filters, Running Totals, Non Distinct plus Distinct Aggregates, OFFSET/FETCH and Sequences.

SQL324: SQL Server Execution Plans – from Compilation to Caching to Reuse

Maciej Pilecki

Execution plan reuse is one of the most important aspects of building well-performing and scalable SQL Server solutions. But it's also the one that is often overlooked during the design phase and becomes very difficult to troubleshoot later. In this session we will discuss in detail the following aspects of SQL Server execution plans: compilation, re-compilation, parameterization, caching, reuse and aging. You will leave this session with full understanding of how to improve your server's performance by increasing execution plan reuse (or how to avoid reuse in case this is necessary).



SQL310: Taking the Sting Out of Statistics

Kimberly L. Tripp

Even if you have the right indexes that doesn't mean that SQL Server's going to use them. Regardless of whether we're talking about adhoc queries, prepared statements or stored procedures - every system has to have accurate statistics in order to function. In this session, I'll explain what statistics are, how they get created, why you might want to add more and how statistics are updated. We'll also look at and understand what is stored with statistics and why it might become out of date as well as how to keep it up to date.

UNDERSTANDING SQL SERVER

SQL227: BLITZ! The SQL - More One Hour SQL Server Takeovers

Brent Ozar

Last year Brent Ozar published a script to quickly assess the health, performance, and security of a SQL Server you've never seen before. He's been steadily refining it, adding more checks and helpful information, and now he's ready to unveil the next generation. You'll learn how to check the three most dangerous threats lurking in servers, how to recognize low-hanging fruit that will instantly improve performance, and get a script that does all this for you. This script makes the life of a production DBA easier.

SQL302: Parallelism and Performance: Are You Getting Full Return on Your CPU Investment?

Adam Machanic

Over the past five years, multi-core processors have made the jump from semi-obscure to commonplace in the data center. While servers with 16, 32, or even 64 cores were once an out-of-reach choice for all except the biggest databases, today we regularly expect such specifications in even our lower-end servers. So, are you getting everything you can out of the wealth of processing power at your disposal? By default, SQL Server automatically handles many of the parallel processing details, but DBAs still need to consider a number of things if they want to ensure that they're taking full advantage. In this session, we will take a detailed look at the ins and outs of how and why SQL Server processes queries in parallel, with examples to help you identify which queries are being processed in parallel and what they're doing. You will then learn the various methods of controlling parallel processing: SQL Server configuration options, the SQL Server 2008 Resource Governor, and query-level hints. The information you take from this session will enable you to immediately evaluate, understand, and improve the state of parallel processing on your servers.

SQL203: Reporting Services Foundations (Part 1)

William R. Vaughn

Reporting Services has taken the industry by storm, with companies all over the world re-evaluating their reporting systems in light of its benefits. Long-time Crystal customers are migrating to Reporting Services en-masse, and need to find the easiest conversion path. This session is designed to bring developers, architects and their managers up to speed on Reporting Services architecture and make the transition as painless as possible. It shows how to properly configure a Reporting Services installation, manage data sources, and protect corporate data. We'll talk about how to get the best performance from your Reporting Services instance as well as how to prevent Trojan attacks, configure SSL security and configure user roles. We'll also discuss the implications and changes imposed by Windows 7 and how to work with them to further enhance security.

SQL206: Reporting Services Foundations (Part 2)

William R. Vaughn

Once developers have installed and configured Reporting Services, it's essential they understand how to use the Report Manager to manage and launch reports, manage subscriptions and snapshots as well as configure other report and data source properties. This session discusses all of the Reporting Services tools as well as how to manage parameters, performance and write RDL-resident expressions – even those written in Visual Basic. NET and other CLR languages. We'll show why it's important to build and manage report snapshots and history as well as how to build a parameter-driven report that need not re-query the data – all to improve performance.

BEST PRACTICES

SQL314: Best Practices for Securing SQL Agent

Andrew Kelly

Too many SQL Server instances have a less than ideal security setup when it comes to SQL Agent jobs but it doesn't have to be that way. We will investigate the various security roles built into SQL Server Agent since 2005 and explain how and when to use each one. We will also concentrate on the Proxy accounts that allow us to define exactly what permissions are needed at the job step level. There are no more excuses for having tasks that are potential security risks in your environment. Come see how quick and easy it is to take control of your SQL Agent jobs.

SQL225: Follow the Rabbit: Wrap-up Q&A

Paul Randal and Kimberly L. Tripp

Now a conference staple, Kimberly and Paul come loaded with slides and highlights from all of their sessions of the conference. If you don't ask questions, they're start adding to the content discussed previously by diving deeper and tying in discussions they've had in breaks, after their sessions and with your questions. This is really YOUR time to ask questions! This session seems unfocused but is often not only informative but highly interactive and fun.

SQL209: Managing Self-Service BI in PowerPivot for SharePoint

Stacia Misner

So your users are clamoring to use PowerPivot for SharePoint, but do you know what it takes to get the environment up and running? In this session, we'll review the architecture to understand what components are required, how they interact, and how workbooks are secured. We'll also discuss how you can use the PowerPivot Management Dashboard to anticipate future capacity requirements by reviewing user activity with popular workbooks, to take appropriate steps to resolve long-running queries, and to monitor dependencies on organizational data sources by analyzing workbook activity.

SQL308: TempDB Best Practices

Andrew Kelly

TempDB is not like your ordinary user database and should not be treated like one. In this session we will explore what makes TempDB different than other databases and why you need to be aware of these differences. Initial configuration is crucial to good performance and we will talk about each of the aspects that potentially affect performance that you should consider up front. We will also spend some time on how to detect the memory and space usage associated with the various users in TempDB along with some common scenarios that you will encounter with a well-used TempDB database. If TempDB suffers then most likely your whole application will suffer as a result. Be proactive and avoid this altogether.

SQL226: Understanding BI Security Best Practices

Stacia Misner

How secure is your BI environment? The Microsoft business intelligence stack contains multiple tools which each have different security configuration options and interdependencies. This session starts with a review of the security architecture of each component in the BI stack and highlights vulnerabilities in the architecture that must be addressed to properly secure your BI environment. In this ses-

sion, you'll also learn about the relationship across the security settings in the BI tools, backend databases, and the Windows operating system. Building on this foundation, you'll learn what steps are necessary to apply security best practices in each component of the Microsoft BI stack.

MONITORING

SQL317: Capturing and Analyzing Perfmon Data

Andrew Kelly

Do you capture performance monitor data in your environment today? If not then why not and if so do you find it tedious and time consuming? Many people find capturing and analyzing large amounts of permon data to be overwhelming and frustrating. This session will show you how you can automate the collection and processing of the perfmon data using built in Windows functions and a handy utility call PAL (Performance Analyzer). See how you can start taking advantage of the wealth of data you can obtain thru perfmon with very little upfront effort.

SQL323: What's Really Happening on Your Server? 15 Powerful SQL Server Dynamic Management Objects

Adam Machanic

There are two kinds of DBAs in this world: those who scratch their heads, unsure of how to find answers, and those who demand real-time, comprehensive insight. This session is for the latter type, the Type A DBAs who are serious about managing their servers as efficiently as possible. The Dynamic Management Objects – a set of views and functions that first shipped with SQL Server 2005 – are a window into the inner workings of your SQL Server instance. Locked within the objects is the information you need to help you solve virtually any performance problem, quickly debug issues as they're occurring, and gain insight into what's actually happening on your server, right now. This session is a fast-paced tour of the ins, outs, whys, hows, and even pitfalls of 15 of the most important views and functions – information gleaned from heavy use of the objects in a number of environments over the past five years. You will learn how to understand transaction behavior, locking, wait statistics, sessions, requests, and much more. No longer will you need to scratch your head, wondering what is slowing down your queries: You will be the master of your SQL Server instance.

TROUBLESHOOTING

SQL422: Advanced Recovery Techniques

Paul Randal

The best way to be able to recover from a disaster is to be prepared! This means you must have practiced some disaster-recovery techniques before being asked to help a customer who is struggling. In this session, Paul will go beyond the simple corruption examples you've already seen and look at some of the less frequently seen issues and advanced techniques, including showing examples of when SQL Server's tools fail.

SQL318: Storage Triage: Troubleshooting Slow Servers

Brent Ozar

Storage pain is like chest pain: maybe it's really dangerous, or maybe it's just heartburn. Microsoft Certified Master and storage specialist Brent Ozar will cover the decision tree he uses to diagnose storage pain. To gain the most out of this session, it'll help to have 3-5 years experience managing databases. You don't have to know internals, but you do need to know the differences between clustered and nonclustered indexes, data and log files, and RAID 5 and RAID 10. You'll learn how to check storage health metrics from inside Windows with DMVs and Perfmon, why the SAN guy keeps saying he doesn't see anything wrong, and how to identify when it really IS a SQL Server problem.

SQL321: Troubleshooting Deadlocks in SQL Server

Maciej Pilecki

Let's face it: in a busy database, deadlock can occur unexpectedly at any time. And what's more troubling, there is no silver-bullet solution to prevent it. Even if you follow every best practice available, it will still happen. So what do you do when it does happen to you? In this session we will cover some of the less-known approaches to avoiding and troubleshooting deadlocks. Using real-life examples, I will show you some of the nastiest deadlocks possible and possible ways to troubleshoot them.

SQL419: Wait Statistics: Avoiding 'Knee-Jerk' Performance Tuning

Paul Randal

One of the first things you should check when investigating performance issues are wait statistics – because SQL Server has a good idea what the problem is. Unfortunately many people misinterpret what SQL Server is telling them and jump to conclusions about how to solve the problem – what Paul calls 'knee-jerk performance tuning'. In this detailed session, Paul will explain and demo many of the most common wait types and show you what they REALLY mean. After attending this session you'll be able to make proper use of this powerful performance tuning technique.

MYTHS AND MISCONCEPTIONS

SQL216: More DBA Mythbusters

Paul Randal

It's amazing how many myths and misconceptions have sprung up and persisted over the years about SQL Server. After 10 years helping people out on forums, newsgroups, and customer engagements, Paul's heard it all. Building on the success of the original DBA Mythbusters session, Paul brings another 75 minutes of myth debunking of a whole new set of myths and misconceptions in this fast-paced session on how SQL Server operates and should be managed and maintained. Come and see how many YOU get right!

SQL320: T-SQL Bug or Feature?

Itzik Ben-Gan

Some behaviors in T-SQL are clear bugs and some are clear features. But being a relational language with many unique aspects compared to procedural languages, sometimes you may find yourself wondering whether a certain behavior is in fact a bug or a feature. This session covers various cases that aren't clear cut and explains why they are considered a bug or a feature. Through those cases the session tries to shed some light on some important principals of this unique language.

DESIGN & ARCHITECTURE

SQL411: Understanding Microsoft SQL Server Memory Usage and Management

Maciej Pilecki

Have you ever wondered why SQL Server seems to be using all the memory on your server? This session seeks to understand why this is, in fact, an expected behavior. The session discusses details of SQL Server internal memory usage and management and its interaction with the operating system. You will understand how SQL Server acquires, uses and releases memory, how to detect memory pressure and bottlenecks and how to properly configure SQL Server memory for different scenarios, especially on servers running other applications

or with multiple instances of SQL Servers. You will leave this session with full understanding of SQL Server memory internals and ready to troubleshoot memory problems in the real world, how to detect memory pressure and bottlenecks and how to properly configure SQL Server memory for different scenarios, especially on servers running other applications or with multiple instances of SQL Servers. We will also cover differences between 32- and 64-bit architectures and why even on a 64-bit machine you can run out of Virtual Address Space.

SQL ServerCentral.com

SQLServerCentral.com TRACK

SSC201: Tips and Tricks for Database Design

Andy Warren

Designing databases is a lot like building the foundation of a house; once it's done it's very hard to change and you live with the results for a very long time! This session focuses on a practical approach to database design. We'll start by reviewing and discussing the rich array of data types and why picking the right data type matters more than you think, and we'll look at our options for ensuring we have good data including defaults, constraints, triggers, and foreign keys. We'll also look at the role of views and synonyms as part of a good design. Then we'll move into a case study of a real-world problem and actually build a database to meet the needs of our customer, who as it turns out wants the best design but can only afford to implement it in phases – more like design in the real world. We'll finish up by reviewing our checklist to make sure we've applied our standards consistently.

SSC202: Top 10 SSRS Best Practices

Andy Warren

Want to get more out of Reporting Services? Make sure that you're doing things the "right" way? This presentation focuses on ten best practices that you can take back to the office and use immediately on your own Reporting Services reports and servers. We will be looking at Reporting Services from the perspectives of the report designer, the testing and QA team, and the DBA as we explore best practices that include defining usable naming standards and layout conventions, planning for Firefox users, tracking report usage, developing a process for moving reports from development to test to production, and more!

SSC203: Top 10 Database Maintenance Best Practices

Brad McGehee

Many DBAs take routine database maintenance for granted. What they don't understand is that the cumulative effect of poor database maintenance can significantly hurt performance and reduce uptime. In this session, you will learn the top 10 key things all DBAs need to know in order to help them maintain their databases at peak performance. In this session you will learn about: Physical File Fragmentation; Database and Log File Management; tempdb Maintenance, msdb Maintenance; Index Maintenance; Statistics Maintenance; Data Corruption Detection; Database and Log File Protection; and Database Maintenance Monitoring.

SSC204: Using SQL Server Compression to Boost Database Performance

Brad McGehee

SQL Server 2008 (including R2) Enterprise Edition offers the ability to compress rows or pages so that more data can be stored on disk and in the data cache. If properly implemented, it not only saves memory and disk space, it also can also boost your databases' performance. In this session, you will learn how row and page compression works, how to implement it, and how to implement compression best practices.

SSC305: Lucky 7: Seven Different Solutions for Bad Parameter Sniffing

Grant Fritchey

Parameter sniffing is a misunderstood issue on SQL Server. Most of the time parameter sniffing is helping performance on your servers. But sometimes, circumstances change and what was helping you is now hurting you, bad. In this session we'll gain an understanding of what exactly parameter sniffing is and why it's usually so helpful. Then, we'll explore how parameter sniffing can go wrong and I'll show you seven different ways you can deal with it when it does. You'll bring back a wealth of knowledge so that you can identify and resolve bad parameter sniffing in your own environment.

SSC206: The SQL Server Optimization Checklist

Grant Fritchey

Squeezing the absolute most performance you possibly can out of your server and databases can be very difficult. It's made even more difficult when you're not starting from a good foundation. This session walks you through a basic set of checks, settings and suggestions that you can use to ensure you're making good choices when configuring your servers and databases. Using this checklist you can avoid common and easily prevented performance issues. Having your servers and databases configured correctly provides a solid foundation upon which you can build your data structures and code. We'll go over information such as memory configurations, standard server settings, data file configurations, and more. All oriented to making sure you take advantage of the hardware you have available.

SSC207: Top 10 SSIS Best Practices

Tim Mitchell

SQL Server Integration Services is a highly versatile product for performing all manner of ETL (Extraction, Transformation, and Loading) operations. Because it is so multifaceted, there are a lot of ways to configure – and misconfigure – the tasks and components within SSIS packages. In this session we'll discuss ten of the best practices for building and configuring SSIS packages. From package configurations to logging and auditing, and naming conventions to deployment, we'll review what works, and why, in real-world SSIS environments. We'll include demos for each of these best practices, along with tales of some less-than-best-practices lessons learned the hard way.

SSC208: Defensive ETL

Tim Mitchell

Dealing with clean data is easy. Unfortunately, most of us don't have that luxury! In the real world, data contains duplicates, inaccuracies, inconsistencies, and other anomalies that can render the information useless to the business. Much like motorists are taught to drive defensively, ETL developers and other data professionals must maintain a "code defensively" attitude to avoid collateral damage from unexpected (and unhandled) occurrences during the ETL process. In this session, we'll discuss some of these pitfalls, including some realistic examples and a few war stories. We'll address some best practices for defensive ETL coding, along with practical demonstrations of these methodologies.

MICROSOFT SESSIONS

Developing Next Generation Windows Applications that Integrate with SharePoint 2010

Migrating Your SharePoint 2010 Applications to the Cloud using Windows Azure

Virtualizing SharePoint 2010 Applications within the Private Cloud

Creating Business Intelligence Dashboards for SharePoint 2010

Building and Deploying Amazing Internet Sites with SharePoint 2010

Exploring the Social Side of SharePoint 2010: From Sites to Search and Beyond

Customizing Office 365 and SharePoint Online Sites using SharePoint Designer

Migrating from SharePoint 2007 to SharePoint 2010

More sessions will be added. Check the website closer to the show date for more details.

SHAREPOINT ADMINISTRATION

HAD01: SharePoint 2010 Search Overview
Matthew McDermott

HAD02: SharePoint 2010 Search Phase 2: Solving Common Search Challenges
Matthew McDermott

HAD03: Enterprise Social Computing with SharePoint 2010
Matthew McDermott

HAD04: Building it Right the First Time; Best Practice SharePoint 2010 Infrastructure Advice
Michael Noel

HAD05: Collaborating with Extranet Partners on SharePoint 2010
Michael Noel

HAD06: SharePoint 2010, Exchange 2010, and Lync 2010; Better Together
Michael Noel

HAD07: Auto-Provisioning of SharePoint Farms using Scripted Intelligence and Server Virtualization
Michael Noel

HAD08: Managing the SharePoint Disruption
Dan Holme

HAD09: Wish I'd Have Known That Sooner! SharePoint Insanity Demystified
Dan Holme

HAD10: Up and Running: Windows PowerShell for SharePoint
Dan Holme

HAD11: Sizing Your Content Databases: Understanding the New Limits
Randy Williams

HAD12: Heavy Metal PowerPivot
Jason Himmelstein and Cornelius J. van Dyk

HAD13: Time Is Money. How SharePoint Logging will Save You Both!
Jason Himmelstein and Cornelius J. van Dyk

SHAREPOINT DEVELOPMENT

HDEV01: How SharePoint Workflow Works ... and How it Breaks
Robert Bogue

HDEV02: Claiming to Get Forms-Based Authentication
Robert Bogue

HDEV03: SharePoint Guidance – Developing Applications – Foundation and Execution
Robert Bogue

HDEV04: Building Silverlight Applications for SharePoint 2010 with MVVM
Andrew Connell

HDEV05: Creating and Using SharePoint 2010 Timer Jobs
Andrew Connell

HDEV06: SharePoint Ribbon Customization Deep Dive
Andrew Connell

HDEV07: Accelerated Introduction to JavaScript for SharePoint Developers
Ted Pattison

HDEV08: Accelerated Introduction to jQuery for SharePoint Developers
Ted Pattison

HDEV09: Developing SharePoint 2010 Solutions with RESTful Services
Ted Pattison

HDEV10: What Happened to Explorer View? Creating Tree and Folder Views for SharePoint 2010 Document Libraries
Scot Hillier

HDEV11: Custom File Upload Solutions for SharePoint 2010
Scot Hillier

HDEV12: Cubes, Scorecards, Charts, and Dashboards Start to Finish in SharePoint 2010
Scot Hillier

NO CODE SOLUTIONS

HNC01: Make the Best Use of SharePoint Designer 2010
Asif Rehmani

HNC02: Create Custom Search Center Solutions without Code
Matthew McDermott

HNC03: Create SharePoint Library Forms Using InfoPath 2010
Asif Rehmani

HNC04: Human Workflow with Visio 2010 and SharePoint Designer 2010
Jason Himmelstein and Cornelius J. van Dyk

OFFICE 365

HOF01: The Evolution of the SharePoint Administrator
Ben Curry

HOF02: Migrating Processes and Content to Office 365
Ben Curry

HOF03: Office 365: Customize SharePoint Online with SharePoint Designer 2010
Asif Rehmani

PRE-PRE-CONFERENCE WORKSHOPS | **SUNDAY, OCTOBER 30, 2011**

WINDOWS Workshop | 9AM - 4PM | Additional Fee: $449

WPR01: The Ultimate Windows Troubleshooting Hands-On Workshop (BRING YOUR OWN LAPTOP)

Bruce MacKenzie-Low

Capitalize on over two decade's worth of troubleshooting experience by spending the day with Bruce Mackenzie-Low as you learn how to troubleshoot the toughest Microsoft Windows outages. Bring your own laptop and get hands-on experience with the Windows Debugger to analyze system and application crashes and hangs. Learn how to configure a system to capture a BSOD (Blue Screen of Death) or force a memory dump from the keyboard. Use state-of-the-art (free) tools from Microsoft to monitor and resolve performance bottlenecks and a variety of application issues. Walk away from this workshop with the confidence and inspiration you'll need to tackle your most challenging Windows outages. This will be THE training session you remember and leverage for years to come! To maximize your learning experience, BYOL (bring your own laptop) running a recent version of Windows, with at least 2GB of free disk space for crashes and with wireless network connectivity. Power strips will be provided in class.

SQL Workshop | 9AM - 4PM | Additional Fee: $399

SPR201: The Foundations of a Healthy SQL Server Database

Kimberly L. Tripp &
Paul Randal

SQL Server is becoming more and more ubiquitous as it underpins many mission-critical enterprise applications like SharePoint, TFS, Dynamics and others. Whether you're using SQL Server as a true data tier or because it just happens to be the data store for an enterprise application, the same common problems can negatively impact database performance. In this workshop we will distill our over 30 years of combined SQL Server experience into a knowledge-packed day where you will learn how to ensure your SQL Server doesn't become your bottleneck. You'll take away a wealth of immediately-applicable practices that you'll be able to understand and use if you're a DBA, a SharePoint administrator, or any IT professional tasked with SQL Server responsibilities. Topics covered will include: data and log file configuration, index fragmentation, tempdb, statistics, integrity checking and more!

PRE-CONFERENCE WORKSHOPS | **MONDAY, OCTOBER 31, 2011**

WINDOWS Workshop | 9AM - 4PM | Additional Fee: $399

WPR02: Running Your Active Directory with Windows Server 2008 R2

Mark Minasi

In the past 11 years, Microsoft's Active Directory has gone from "it'll never beat Novell" to being the number one directory service in the IT world. Thus, there's a pretty good chance that your company has an AD and, if you're attending this conference, as nearly as good a chance that you're one of the people running that AD. But are you getting as much out of that AD as you might? Attend this fast, fun, informative one-day workshop with AD expert and bestselling author Mark Minasi to find out. In this essential class, Mark shows you how to take your AD management skills to the next level.

In this workshop, you'll see how to make use of some powerful but unfortunately obscure built-in AD diagnostic tools, like netlogon debug logs and advanced DNS logs. You'll take diagnostics further with DIG, the far-superior (and free) replacement for nslookup. You'll see how to save money AND avoid AD troubles by finally understanding whether or not it's safe to virtualize domain controllers (it IS, as you'll learn, despite a lot of anti-DC-virtualization FUD on the Net) and the simple procedures you'll need to know to make it work without trouble.

EXCHANGE Workshop | 9AM - 4PM | Additional Fee: $399

EPR01: Preparing for Exchange 2010

Tony Redmond &
Paul Robichaux

Learn all you need to prepare to deploy Exchange 2010 on-premises or in the cloud with Office 365 in this one-day seminar based on material extracted from the popular "Exchange 2010 Maestro" series. The workshop will be presented by MVPs and acknowledged Exchange experts Paul Robichaux and Tony Redmond (author of **Exchange 2010 Inside Out** - Microsoft Press). Both write frequently about Exchange for ***Windows IT Pro*** magazine and over six hours, they will discuss:

- A review of all of the major new features and other product enhancements in Microsoft Exchange 2010 and why and how these advances can add value to your company
- Client options for Exchange 2010
- The tools available from Microsoft and other companies to help you deploy Exchange 2010
- Critical factors in the decision whether to deploy on-premises or in the cloud - or whether a hybrid deployment is best
- How to approach the migration to Exchange 2010

The workshop will be fully updated to include the latest version of Exchange 2010 available at the time of the event (expected to be Exchange 2010 SP2).

SHAREPOINT Workshop | 9AM - 4PM | Additional Fee: $399

HPR02: Dan Holme's SharePoint Administration and Configuration MasterClass

Dan Holme

Get up and running in SharePoint 2010 with this full-day preconference workshop. You will learn the best practices for building an effective, secure, and scalable SharePoint farm, from the ground up, and you will leave with a prescriptive guide to a successful SharePoint 2010 implementation. This workshop is aimed squarely at enterprises that are new to SharePoint, are migrating from previous versions, or are trying to clean up and optimize a chaotic SharePoint environment. You'll start with best practice, scripted deployment to automate server and farm provisioning. You'll build an effective logical architecture of farms, web applications, site collections, and content databases. You'll deploy key services, including search, metadata, and user profiles. You'll create a structure for a variety of scenarios, including intranet, collaboration, extranet, and applications.

PRE-CONFERENCE WORKSHOPS | MONDAY, OCTOBER 31, 2011

SQL SERVER Workshops | 9AM - 4PM | Additional Fee: $399

SPR202: Collaborative Business Intelligence: Putting the Pieces Together

Stacia Misner

As individual products, SQL Server 2008 R2, SharePoint 2010, and Excel 2010 expand your options for enabling BI in your organization, but collectively they create a solid platform for collaborative BI. Getting the configuration just right and knowing which tool to use for which job can be tricky. Come to this session to learn how to create a collaborative BI solution that provides a central location for administrators to organize and manage information assets and for users to locate, analyze, and personalize information available from SSAS, SSRS, PerformancePoint, PowerPivot, and other sources. In this workshop, we'll review the technical architecture required to support collaborative BI and walk through the construction of a collaborative BI solution.

NOTE: LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS. THE COST OF A WORKSHOP IS IN ADDITION TO THE REGULAR CONFERENCE FEE.

SPR303: Designing for Performance and Scalability

Kimberly L. Tripp

If you don't design with performance and scalability in mind, inevitably your databases will reach a point where scaling up the amount of data or users causes performance to decrease. There are many things to consider during the initial design that can help avoid this, and there are things you can do to existing designs that can help fix this. For a SQL Server system to be truly scalable you need to understand three key points: the data being stored, the workload that's accessing the data and how SQL Server works, to some degree. This last part is what's often missing. SQL Server is a general purpose relational database management system and as such it can do ANYTHING. However, it's not necessary optimal (using defaults) for everything. Even the most common way that people partition, using table partitioning, isn't always the most effective. This workshop is all about the structures and what's necessary for them to scale and I'll cover partitioning in transaction processing as well as decision support. Often partitioning is needed in both but the design can be drastically different. Finally, I'll compare and contrast why filtering (filtered indexes and filtered stats) can solve some problems but partitioning can solve more.

POST-CONFERENCE WORKSHOPS | FRIDAY, NOVEMBER 4, 2011

WINDOWS Workshop | 9AM - 4PM | Additional Fee: $399

WPS01: Wireless for the IT Professional – Everything You Need to Know (Most of Which You're Doing Wrong)

Mike Danseglio & Dr. Avril Salter

The vast majority of organizations use wireless networking to meet the needs of mobile users, portable devices, and other demands of modern business. But few stop to think about exactly how this technology works. They simply deploy the latest standard with the highest security settings and assume that's appropriate. But nothing could be further from the truth. Using the appropriate frequency, channel, signal strength, encryption, and other settings makes the difference between a fast, stable network and one that is a chore to use and manage. In this full day workshop, you'll learn everything you need to know about wireless technology. Starting at the beginning, Dr. Avril Salter will explain how wireless works from the ground up (no pun). She explains the difference in frequencies, channels, signal types, MIMO, and more, and how all of these factors impact wireless networking. She will demonstrate conducting a wireless site survey that any IT professional can do to show how this simple but critical step can help prevent many wireless issues during deployment. Dr. Salter will use tools and techniques during the session that you can apply to most environments without breaking the bank. Once you have a firm grasp of the core "radio" component, Dr. Salter is joined by Mike Danseglio, an expert in Windows-based networking. Mike and Avril will demonstrate the entire wireless planning, deployment, and operations lifecycle for a Windows-based environment. Mike will also demystify topics that are common points of frustration such as 802.1X port-based and directory-based authentication, using Windows as a RADIUS server, configuring Windows wireless networking for a seamless experience, and more. Throughout this entire session you will see hands-on demonstrations that help you learn how to apply the techniques and tools to ensure that your wireless network remains fast, stable, and secure.

SQL SERVER Workshops | 9AM - 4PM | Additional Fee: $399

SPS401: Advanced T-SQL for SQL Server 2008 and Denali

Itzik Ben-Gan

You're a T-SQL developer or DBA and you learned most of what you know about T-SQL by the seat of your pants. You can handle day-to-day T-SQL querying and programming tasks in a reasonable manner, but you're looking for better and more efficient solutions. This workshop is for you. It covers common T-SQL querying and programming tasks and shows polished, optimal techniques to handle those. Some of the techniques that you will learn in this seminar are very recent developments. You will learn how to utilize T-SQL constructs available in SQL Server 2008 in creative and efficient ways. You will also learn new T-SQL features planned in the next major release of SQL Server–code-named Denali. There are lots of exciting new T-SQL features planned in SQL Server Denali–some quite profound–and knowing about them ahead can make you better prepared, affecting how you write code today.

SPS402: Practical Performance Monitoring

Andrew Kelly

When it comes to performance problems in SQL Server where do you start? We will cover the techniques that you can use immediately in your environment to get going in the right direction when it comes to finding performance issues. We will focus on the most practical aspects of performance monitoring and performance issues that most DBAs will encounter in their daily routines. There will be ample demos to highlight the key performance problems along with code that you can take back and use to find the performance issues in your own environment. Take the practical approach to finding performance problems in SQL Server and spend less time chasing your tail.

ONLY MICROSOFT AND INDUSTRY EXPERTS SPEAK AT CONNECTIONS!

KEVIN ALLISON
MICROSOFT

CHRIS AVIS
MICROSOFT

ITZIK BEN-GAN
SOLID QUALITY LEARNING

ROBERT BOGUE
THOR PROJECTS

QUENTIN CLARK
MICROSOFT

ANDREW CONNELL
CRITICAL PATH TRAINING

BEN CURRY
SUMMIT 7 SYSTEMS

MIKE DANSEGLIO
CONCENTRATED TECHNOLOGY

BRIAN DESMOND
MORAN TECHNOLOGY CONSULTING

STEVE FOX
MICROSOFT

GRANT FRITCHEY
RED GATE SOFTWARE

JASON HIMMELSTEIN
RAYTHEON COMPANY

DAN HOLME
AVEPOINT

SIEGFRIED JAGOTT
SIEMENS

ANDREW KELLY
SOLID QUALITY LEARNING

WILLIAM LEFKOVICS
MOJAVE MEDIA GROUP, LLC

ADAM MACHANIC
DATA MANIPULATION GROUP, INC.

BRUCE MACKENZIE-LOW
HP

ROMI MAHAJAN
MICROSOFT

RUI MAXIMO
MICROSOFT

JIM MCBEE
ITHICOS SOLUTIONS

MATTHEW MCDERMOTT
APTILLON

BRAD MCGEHEE
RED GATE TECHNOLOGY

TIM MCMICHAEL
MICROSOFT

MARK MINASI
MINASI RESEARCH AND DEVELOPMENT

STACIA MISNER
DATA INSPIRATIONS

TIM MITCHELL

JEREMY MOSKOWITZ
MOSKOWITZ, INC.

MICHAEL NOEL
CONVERGENT COMPUTING

BRENT OZAR
BRENT OZAR PLF, INC.

TED PATTISON
CRITICAL PATH TRAINING

MACIEJ PILECKI
PROJECT BOTTICELLI

PAUL S. RANDAL
SQLSKILLS.COM

TONY REDMOND
TONY REDMOND AND ASSOCIATES

ASIF REHMANI
SHAREPOINT-ELEARNING.COM

ALAN SUGANO
ADS CONSULTING GROUP

DR. AVRIL SALTER
CELLSTREAM, INC.

MICHAEL B. SMITH
THE ESSENTIAL EXCHANGE

JEFFREY SNOVER
MICROSOFT

BYRON SPURLOCK
QUADRAN-TECHNOLOGIES

KIMBERLY L. TRIPP
SQLSKILLS.COM

CORNELIUS J. VAN DYK

WILLIAM R. VAUGHN
BETA V CORPORATION

ANTHONY VITNELL
DIMENSION DATA

ANDY WARREN
CONSULTANT

RANDY WILLIAMS
AVEPOINT

And many more...
Check our Web site as we continue to update it with speaker pictures and bios!

Join us!

LAS VEGAS, NEVADA | MANDALAY BAY RESORT & CASINO
OCTOBER 31-NOVEMBER 3, 2011

Enjoy the excitement of a premiere Las Vegas hotel!

Positioned at the south end of The Strip, Mandalay Bay Resort and Casino offers elegance, excitement and escape. Enjoy its restaurants, entertainment and enormous beach-pool, as well as wireless Internet in your room and optional VIP access to shows, restaurants, the spa and more.

HOTEL ACCOMMODATIONS

Mandalay Bay Resort and Casino, 3950 Las Vegas Blvd. South, Las Vegas, Nevada, is the conference site and host hotel. SPACE IS LIMITED so reserve your room early by calling the conference hotline at 800-438-6720 or 203-400-6121.

TAX DEDUCTION

Your attendance to a WinConnections conference may be tax deductible. Visit www.irs.ustreas.gov. Look for topic 513 - Educational Expenses. You may be able to deduct the conference fee if you undertake to (1) maintain or improve skills required in your present job; (2) fulfill an employment condition mandated by your employer to keep your salary, status, or job.

GROUP DISCOUNT

Register individuals from one company at the same time and receive a group discount.

Call 800-438-6720 to take advantage of group discount pricing.

CAR RENTAL

Hertz is offering auto rental discounts to attendees. Call the Hertz Meeting Desk at 800-654-2240 for reservations and refer to code CV# 010R0046 (Hertz) under Connections Vegas to receive your attendee discount.

ATTIRE

The recommended dress for the conference is casual and comfortable. Please bring along a sweater or jacket, as the ballrooms can get cool with the hotel's air conditioning.

SPONSORSHIP/EXHIBIT INFORMATION

For sponsorship information,
contact Rod Dunlap
480-917-3527 phone
E-mail rod@devconnections.com

See websites for more details.
www.WinConnections.com
www.DevConnections.com

Notes & Policies: The Conference Producers reserve the right to cancel the conference by refunding the registration fee. Producers can substitute speakers and topics and cancel sessions without notice or obligation. Updates will be posted on our website at www.WinConnections.com. Tape recording, photography is not allowed at any session. Conference producers will be taking candid pictures of events and reserve the right to reproduce. By attending this conference you agree to this policy. You may transfer this registration to a colleague by notifying us before the start of the event. Please inform us if you have any special needs or dietary restrictions when you register. The conference registration includes the following subscriptions. This is not an additional expense and subtraction from prices listed is not permissible. Windows, Exchange and Unified Communications Connections registration includes a one-year (12 issues) print subscription to ***Windows IT Pro*** magazine for Exchange and Windows conference attendees only. Current subscribers will have an additional 12-months added to their subscription. Subscriptions outside of the United States will be served in digital; $12.50 of the funds will be allocated toward a subscription to ***Windows IT Pro*** ($49.95 value).

Registration & Cancellation Policy: Registrations are not confirmed until payment is received. Cancellations before September 28, 2011 must be received in writing and will be refunded minus a $100 processing fee. After September 28, 2011 cancellations and no shows are liable for full registration; it can be transferred to the next Conference within 12 months or to another person. Microsoft, Microsoft .NET, ASP.NET, Visual Studio.NET, Microsoft SQL Server, Exchange and Windows are either trademarks or registered trademarks of Microsoft Corporation. All other trademarks are property of their owners.

CONFERENCE REGISTRATION • OCTOBER 31 TO NOVEMBER 3, 2011

FULL CONFERENCE REGISTRATION INCLUDES KEYNOTE ON OCTOBER 31, 2011
THROUGH CLOSING SESSION NOVEMBER 3, 2011 4:30PM

NAME _____ PRIORITY CODE _____

COMPANY _____ TITLE _____

STREET ADDRESS (REQUIRED TO SHIP MATERIALS) _____

CITY, STATE, POSTAL CODE _____ COUNTRY _____

TELEPHONE _____ FAX _____ E-MAIL ADDRESS (IMPORTANT) _____

ONLINE: www.WinConnections.com
E-MAIL: info@WinConnections.com
PHONE: (800) 438-6720
(203) 400-6121
FAX: (913) 514-9362
MAIL:
Penton Media
731 Main Street, Suite C3
Monroe CT 06468

CHECK THE CONFERENCE YOU ARE REGISTERING FOR. NOTE THAT YOU CAN ATTEND ANY OF THE CO-LOCATED CONFERENCES FOR NO ADDITIONAL CHARGE.

☐ **Windows Connections** ☐ **Microsoft Exchange Connections & UC Connections**
☐ **SharePoint Connections** ☐ **SQL Server Connections**

On or Before SEPTEMBER 19, 2011 ..... $1495 _____
After SEPTEMBER 19, 2011 ..... $1595 _____

PRE-PRE-CONFERENCE WORKSHOP SUNDAY, OCTOBER 30, 2011 LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS.

☐ WPR01: THE ULTIMATE WINDOWS TROUBLESHOOTING HANDS-ON WORKSHOP MACKENZIE-LOW ..... 9AM - 4PM ..... $449 _____
BRING YOUR OWN LAPTOP

☐ SPR201: THE FOUNDATIONS OF A HEALTHY SQL SERVER DATABASE TRIPP & RANDAL ..... 9AM - 4PM ..... $399 _____

PRE-CONFERENCE WORKSHOPS MONDAY, OCTOBER 31, 2011 LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS.

☐ EPR01: PREPARING FOR EXCHANGE 2010 REDMOND & ROBICHAUX ..... 9AM - 4PM ..... $399 _____
☐ WPR02: RUNNING YOUR ACTIVE DIRECTORY WITH WINDOWS SERVER 2008 R2 MINASI ..... 9AM - 4PM ..... $399 _____
☐ SPR202: COLLABORATIVE BUSINESS INTELLIGENCE: PUTTING THE PIECES TOGETHER MISNER ..... 9AM - 4PM ..... $399 _____
☐ SPR303: DESIGNING FOR PERFORMANCE AND SCALABILITY TRIPP ..... 9AM - 4PM ..... $399 _____
☐ HPR02: DAN HOLME'S SHAREPOINT ADMINISTRATION AND CONFIGURATION MASTERCLASS HOLME ..... 9AM - 4PM ..... $399 _____

POST-CONFERENCE WORKSHOPS FRIDAY, NOVEMBER 4, 2011 LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS.

☐ WPS01: WIRELESS FOR THE IT PROFESSIONAL – EVERYTHING YOU NEED TO KNOW (MOST OF WHICH YOU'RE DOING WRONG) DANSEGLIO & SALTER ..... 9AM - 4PM ..... $399 _____
☐ SPS401: ADVANCED T-SQL FOR SQL SERVER 2008 AND DENALI BEN-GAN ..... 9AM - 4PM ..... $399 _____
☐ SPS402: PRACTICAL PERFORMANCE MONITORING KELLY ..... 9AM - 4PM ..... $399 _____

CONFERENCE MATERIALS

FULL CONFERENCE REGISTRATION INCLUDES MATERIALS FOR THE CONFERENCE FOR WHICH YOU REGISTER; YOU MAY PURCHASE MATERIALS FOR THE OTHER CONCURRENTLY RUN EVENTS.

☐ MICROSOFT EXCHANGE CONNECTIONS CD ..... $50 _____
☐ WINDOWS CONNECTIONS CD ..... $50 _____
☐ SHAREPOINT CONNECTIONS CD ..... $50 _____
☐ SQL SERVER CONNECTIONS CD ..... $50 _____

TOTAL _____

☐ CHECKS (payable to Penton Media) All payments must be in US Currency. Checks must be drawn on a US bank.

☐ CREDIT CARD ☐ VISA ☐ MASTERCARD ☐ AMEX

CREDIT CARD NO. _____ EXPIRATION DATE _____

Cardholder's Signature _____ Cardholder's Name (print) _____

Penton Media
c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 06468

Mailroom: If addressee is no longer here,
please route to MIS Manager or Training Director

FOLLOW US!
twitter.com/
winconnect

FIND US!
facebook.com/
winconnections

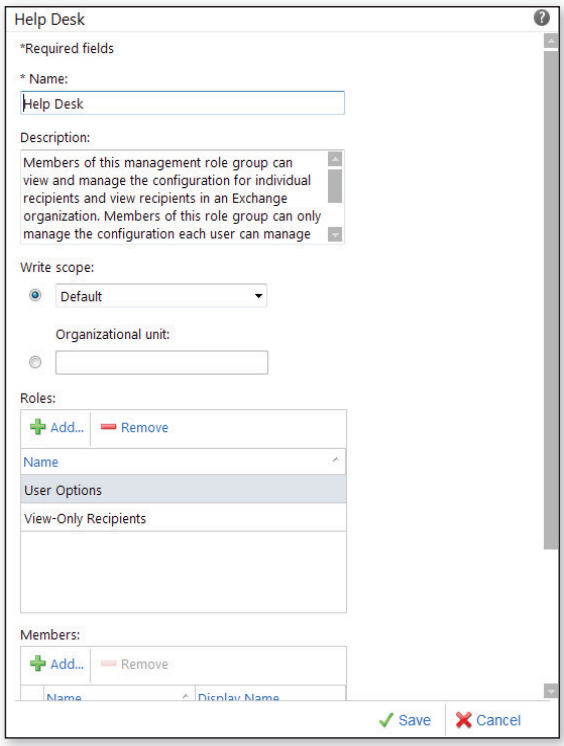


Figure 4: Managing the Help desk RBAC role group

large amounts of Exchange administrator time. With Exchange 2010, multi-mailbox searches can be delegated to a legal department user who can perform searches (and place litigation holds on mailboxes) without the intervention of an Exchange administrator. (For more information about Exchange 2010's multi-mailbox search functionality, see "Multi-Mailbox Search in Exchange Server 2010," July 2010, InstantDoc ID 125260.)

Finally, the Delivery Reports interface in Figure 3 has an additional field to filter on the message sender when accessed by users with elevated permissions. This gives delegated administrators or service desk analysts the ability to track a message when they receive an end-user request for assistance in determining the fate of a message. Previously, this common request required escalation to an Exchange administrator.

Administrator Functionality

Finally, the ECP includes important functionality for Exchange administrators. Unfortunately, the ECP introduced some confusion in terms of where certain tasks need to be performed. The vast majority of configuration tasks are possible only through the Exchange Management Console (EMC); however, several tasks are possible either through both the EMC and ECP or possible only through the ECP.

Tasks that are possible only through the ECP include management of RBAC settings, management of group naming conventions, management of Microsoft ActiveSync device quarantine, and execution of various auditing reports. Some additional tasks are also possible through the EMC, such as configuration of transport and journal rules and ActiveSync policies and message tracking. Of course, the mailbox and group management tasks that I discussed earlier are also possible through the EMC.

Exchange 2010 SP1 greatly improved the RBAC management functionality in the ECP and substantially reduced the need to perform RBAC tasks through the Exchange Management Shell (EMS). The most common tasks, such as managing the membership of a role group or creating a new role group, are now possible graphically. Roles can be added to role groups, and you can tweak the scope (e.g., organizational unit—OU) and membership of a role group, as Figure 4 shows.

Group naming conventions is another new feature in Exchange 2010 SP1. This feature is accessible only through the ECP. You can use the group naming conventions feature to enforce policies on groups that users are allowed to create through the ECP. You can apply policies such as including a prefix for all group names or requiring that the user's department be included in the name of the group (e.g., you might want all your groups to start with DL- and to include the department of the user creating the group, such as DL-IT- for a group created by a user in the IT department). You can also define blocked words that can't be included in a group's name.

Exchange 2010 includes a feature known as ActiveSync Device Access Rules, which lets administrators manage the types of mobile devices that are allowed to connect to Exchange. Configuration for this functionality is accessible in the ECP by selecting the Manage My Organization view, then selecting Phone & Voice, ActiveSync Access. You can use this feature to limit access based on a device's make and model. Based on this information, you can allow, block, or quarantine devices that connect for the first time. Devices that are quarantined require administrator approval to synchronize. Unfortunately, the granularity of the make and model information isn't standardized and varies based on the implementation of ActiveSync. Each vendor that implements the ActiveSync protocol can choose what information to provide in the make and model fields, as well as how to format the information.

Exchange 2010 SP1 improves auditing, making it much easier to report on the data collected by the auditing processes. Several reports are included and can be accessed through the ECP (e.g., reviewing administrator audit logs and mailbox access reports). The reports that can be exported in text or XML formats aren't particularly granular and might contain too much data. Therefore, the various PowerShell cmdlets (e.g., Search-AdminAuditLog) associated with these reports might be a much better solution.

Beyond the EMC

Exchange Server 2010's ECP is a new web interface that provides a great deal of flexibility for end users, technicians, delegated administrators, and Exchange administrators. You can use the ECP to manage numerous Exchange features, including most mailbox options. Some Exchange features that aren't exposed in the EMC have a web-based UI in the ECP, which limits the number of tasks that are accessible only through PowerShell.

InstantDoc ID 135908

Brian Desmond
(brian@briandesmond.com) is a Directory Services MVP and senior consultant for Moran Technology Consulting in Chicago. Brian is author of *Active Directory*, 4th edition (O'Reilly), and blogs at www.briandesmond.com. He wrote this article on a plane to Seattle.

Calculate MD5 and SHA1 File Hashes Using PowerShell

An easy-to-use tool lets you verify the integrity of downloaded files

by Bill Stewart

The majority of software distribution occurs electronically. However, the larger the downloads, the larger the risk of corrupted data transfer. Hence, it's very useful to be able to verify the integrity of downloaded files. Cryptographic hashing algorithms provide one way to do this. A hashing algorithm takes a series of bytes (such as the bytes of a file), performs a calculation using those bytes, and produces an output value of a fixed size (e.g., 128 bits, 160 bits). The goal of these hashing algorithms is that no two inputs should produce the same output. Two common hashing algorithms are the Message Digest 5 Algorithm (MD5) and Secure Hash Algorithm-1 (SHA1). These algorithms have been shown to contain flaws (i.e., there's the possibility that two different inputs can produce the same output), but they're robust enough to verify file integrity in the vast majority of cases.

Figure 1 and Figure 2 show practical examples of hash values. Figure 1 shows an SHA1 hash value for an .iso file on Microsoft TechNet. Figure 2 shows two MD5 hash values for OpenOffice.org installers. If you download these files, you can calculate the SHA1 or MD5 hash values to verify whether the files downloaded without any data corruption.

Introducing Get-FileHash.ps1

Microsoft doesn't provide a command to calculate hash values for files, so I decided to write a Windows PowerShell script, Get-FileHash.ps1, that calculates MD5 or SHA1 hash values for files using the Microsoft .NET Framework. The script requires PowerShell 2.0 or later. You can download it by going to www.windowsitpro.com, entering 139518 in the InstantDoc ID text box, and clicking the 139518 .zip hotlink. I recommend placing the Get-FileHash.ps1 file in a directory in your path.

To execute the script, follow the syntax

```
Get-FileHash [-Path] <String[]>
  [-HashType <String>]
```

or

```
Get-FileHash -LiteralPath <String[]>
  [-HashType <String>]
```

The -Path parameter name is optional and specifies one or more files for which you want to output a hash value. Wildcards are permitted. The script will accept pipeline input in place of the -Path parameter.

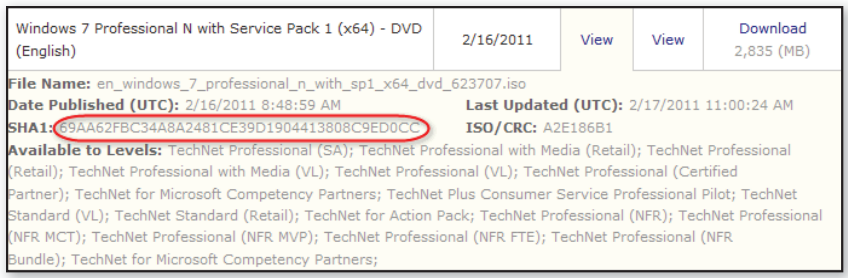


Figure 1: An SHA1 hash value for an .iso file

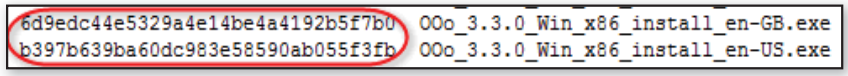


Figure 2: MD5 hash values for OpenOffice.org installers

If you want to specify the name of a file that contains characters that PowerShell normally interprets as escape characters (e.g., the square bracket characters [and]), you can use the -LiteralPath parameter and one or more filenames. If you use -LiteralPath, you can't use wildcards and the script will ignore pipeline input. Note that the -Path and -LiteralPath parameters are mutually exclusive.

The -HashType parameter's value must be the string *MD5* or *SHA1*. If you omit -HashType, MD5 is the default.

Get-FileHash.ps1 outputs objects containing each file's path and its MD5 or SHA1 hash value. Figure 3 shows a sample command and its output. In this command, the filenames are being provided through pipeline input.

Understanding the Script

Get-FileHash.ps1 uses two features new to PowerShell 2.0 and later: Comment-based help and advanced function parameters. Comment-based help enables the Get-Help cmdlet to display help information for the script. Advanced function parameters allow the script to behave like a cmdlet.

Comment-based help is a series of comment lines (lines beginning with #) or a comment block (text enclosed between <# and #>) that contains special keywords that PowerShell uses to generate help information. If you use the command

```
Get-Help Get-FileHash
```

PowerShell uses the special keywords (e.g., .SYNOPSIS, .DESCRIPTION, .PARAMETER) to generate the help text. Comment-based help is a great addition to PowerShell 2.0 that makes it very easy to self-comment functions and scripts. Run the command

```
Get-Help about_Comment_Based_Help
```

at a PowerShell prompt for more information about how to use comment-based help.

Advanced parameters cause PowerShell to use cmdlet-like rules for parsing the script's command-line parameters. Get-FileHash.ps1 uses parameter sets, which enable the script to accept mutually exclusive parameters.

Listing 1 shows Get-FileHash.ps1's CmdletBinding attribute and param statement. CmdletBinding enables cmdlet-like behavior for the script's parameters and specifies the default parameter set. The param statement contains three parameters, which are declared with Parameter statements. Each Parameter statement includes attributes that establish the parameter's behavior. The attributes are as follows:

- ParameterSetName="Name": Specifies the parameter set to which the parameter belongs (either Path or LiteralPath). If a parameter doesn't specify a parameter set, it's valid for any parameter set. The ParameterSetName property of the $PSCmdlet object contains the current parameter set name.
- Position=n: The parameter's position on the command line. Position=0 means the parameter must appear first, Position=1 means the parameter must appear second, and so forth.
- Mandatory=$TRUE: Specifies that the parameter is required. If the parameter isn't specified, PowerShell will prompt for input for the parameter.
- ValueFromPipeline=$TRUE: Specifies that the parameter's input can come from the pipeline.

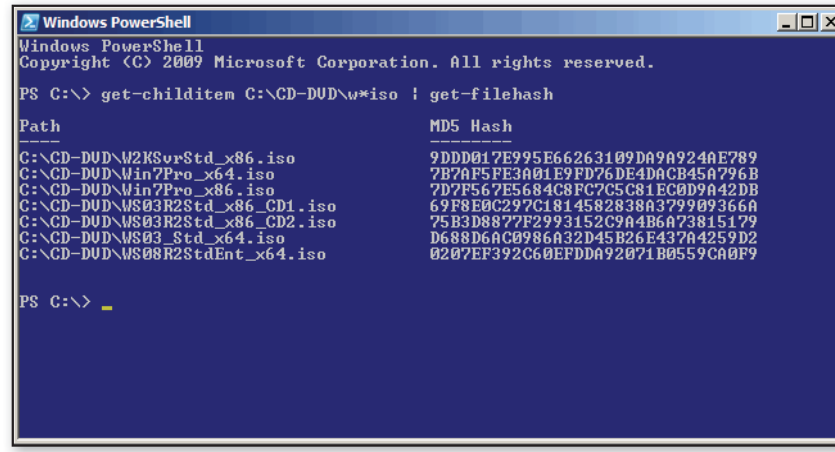


Figure 3: Sample command and its output

Listing 1: The CmdletBinding Attribute and param Statement

```
[CmdletBinding(DefaultParameterSetName="Path")]
param(
  [Parameter(ParameterSetName="Path",Position=0,Mandatory=$TRUE,
    ValueFromPipeline=$TRUE)]
    [String[]] $Path,
  [Parameter(ParameterSetName="LiteralPath",Position=0,Mandatory=$TRUE)]
    [String[]] $LiteralPath,
  [Parameter(Position=1)]
    [String] $HashType="MD5"
)
```

Learning Path

For more information about MD5 and SHA1:

"MD5 Collisions Put PKI At Risk," InstantDoc ID 101145

"Need to Reverse An MD5 or SHA1 Hash To Plain Text?" InstantDoc ID 97925

"Q: Can the default encryption types the Kerberos authentication protocol uses in Windows 7 and Windows Server 2008 R2 cause compatibility problems? Is there a workaround?" InstantDoc ID 125072

For more scripting articles by Bill Stewart:

"Auditing 32-Bit and 64-Bit Applications with PowerShell," InstantDoc ID 136129

"Byte Conversions Made Easy," InstantDoc ID 129737

"Replacing Strings in Files Using PowerShell," InstantDoc ID 126454

"Running PowerShell Scripts Is as Easy as 1-2-3," InstantDoc ID 103427

"Take Control of the PowerShell Console's Colors," InstantDoc ID 103573

"Windows PowerShell 2.0 Remoting," InstantDoc ID 125470

For more information about these attributes, run these commands at a PowerShell prompt:

```
Get-Help about_Functions_Advanced
Get-Help
  about_Functions_Advanced_Parameters
Get-Help
  about_Functions_
  CmdletBindingAttribute
```

(Although the last two commands wrap here, you'd enter each command on one line in the PowerShell console.)

After the param statement, Get-FileHash.ps1 uses the begin and process scriptblocks to carry out the script's cmdlet-like behavior. The begin scriptblock executes once before the pipeline processing, and the process scriptblock executes once for each pipeline item. If there is no pipeline input, the begin and process scriptblocks each execute once.

Listing 2: The get-filehash2 Function

```
# Returns an object containing the file's path and its hash as a hexadecimal string.
# The Provider object must have a ComputeHash method that returns an array of bytes.
function get-filehash2($file) {
  if ($file -isnot [System.IO.FileInfo]) {
    write-error "'$($file)' is not a file."
    return
  }
  $hashstring = new-object System.Text.StringBuilder
  $stream = $file.OpenRead()
  if ($stream) {
    foreach ($byte in $Provider.ComputeHash($stream)) {
      [Void] $hashstring.Append($byte.ToString("X2"))
    }
    $stream.Close()
  }
  "" | select-object @{Name="Path"; Expression={$file.FullName}},
    @{Name="$($Provider.GetType().BaseType.Name) Hash";
      Expression={$hashstring.ToString()}}
}
```

Inside the begin scriptblock, the script validates that the -HashType parameter is either MD5 or SHA1 and creates the $Provider variable, which contains the .NET cryptography object that computes file hashes. Next, the script determines whether the -Path parameter appears on the command line and whether it's bound. If the -Path parameter is present but not bound, the script assumes the input will be coming from the pipeline and sets the $PIPELINEINPUT variable to true.

The begin scriptblock also contains the get-filehash2 function, which is really the workhorse function of the script. I'll describe the get-filehash2 function in a moment.

Inside the process scriptblock, the script checks to see whether the Path parameter set is active (i.e., the -Path parameter was used). If the Path parameter set is active, the script checks the $PIPELINEINPUT variable's value to determine whether it should take input from the pipeline or from the content of the -Path parameter. If there is pipeline input, the script executes the get-filehash2 function for each input object. If there is no pipeline input, the script uses the Get-Item and ForEach-Object cmdlets to send input to the get-filehash2 function.

If the Path parameter set isn't active (meaning LiteralPath is the active parameter set), the script uses the Get-Item cmdlet with its -LiteralPath parameter to retrieve the file. If the Get-Item cmdlet succeeds (that is, the $file variable isn't empty), the script passes the $file variable as a parameter to the get-filehash2 function.

The get-filehash2 Function

As I mentioned previously, the get-filehash2 function, shown in Listing 2, is the workhorse function of the script. It performs three tasks:

1. It validates whether the $file parameter's value is really a file. This is necessary because PowerShell paths can refer to items other than files, such as registry subkeys and directories.
2. It calculates the file's MD5 or SHA1 hash value. The function calls the cryptographic provider's ComputeHash method, which calculates a hash value based on a stream of bytes (in this case, the contents of a file). This result is returned as a string of bytes, so the function uses the .NET StringBuilder object to build a string containing these bytes as a hexadecimal string.
3. It outputs a custom object containing the file's full name and its hash value. The function uses the Select-Object cmdlet to output this custom object.

File Hashing Made Easy

Get-FileHash.ps1 places the power of the .NET Framework's MD5 and SHA1 file hashing algorithms at your fingertips. With Get-FileHash.ps1, you're no longer bereft of an easy-to-use tool for calculating MD5 and SHA1 file hashes from the PowerShell command line.

InstantDoc ID 139518

Bill Stewart
(bstewart@iname.com) is a scripting guru who works in the IT infrastructure group at Emcore in Albuquerque, New Mexico. He has written numerous articles about Windows scripting, is a moderator for Microsoft's Scripting Guys forum, and offers free tools on his website at westmesatech.com.

PDF Malware Mitigation

Protect against a multitude of PDF vulnerabilities

by Didier Stevens

The PDF file format is very popular. This page-description language and the PDF reader applications that support it are designed to prevent arbitrary code execution. However, numerous vulnerabilities have been found in popular PDF readers and exploited by countless malicious PDF documents. In this article, I explain how malicious PDF documents can execute arbitrary code, as well as what you can do as an administrator to protect your users. Many of the mitigation techniques that I discuss also apply to other applications, such as Microsoft Office documents.

Figure 1 shows the PDL code for a very simple one-page PDF document with the text "Hello World." I designed it to contain only the most essential elements that make up a PDF document and to use only ASCII characters, so that you can read the internals of the document.

A PDF document contains a tree structure of objects with all the instructions needed by the PDF reader to render the document's pages. In our example, the root object is 1 (1 0 obj) and is found at absolute position 12. The root object refers to the collection of pages found in the PDF document (i.e., object 3). Our example document contains only one page, defined in object 4. The content of the page is defined in object 5; you can find the text Hello World between parentheses. (The other keywords define text properties, such as the font to be used and its location on the page.)

This PDF example is easy to understand, because it uses uncompressed text. Typically, PDF documents use compressed text and can't be easily read without appropriate tools.

The PDF language and most PDF readers support JavaScript. Scripts can be embedded inside a PDF document and executed by the JavaScript engine of the PDF reader. This engine is restricted in its interaction with the OS. For example, there are no JavaScript statements or functions that allow arbitrary files to be read from or written to. JavaScript in PDF documents is often used in form processing, such as in order forms to calculate totals and sales tax.

So, how do malware authors create PDF documents that infect systems? They do so by exploiting bugs (vulnerabilities) that they actively research in popular PDF reader applications, such as Adobe Reader. These vulnerabilities are often found in the PDF engine or in the JavaScript engine. Back in 2008, one such vulnerability was found in Adobe Reader in the JavaScript util.printf function. (Adobe patched this vulnerability, and it doesn't exist in recent versions of Adobe Reader.)

Util.printf is a function that takes arguments and produces a formatted string according to the arguments passed to it. But when util.printf is passed some very specific arguments, a bug in the internal code of the util.printf function is triggered. When called with these arguments, the internal code of util.printf doesn't behave as the programmers intended, because of a bug. Instead of formatting text and returning execution, the program flow makes the execution of the internal code jump outside the program, at an address where no code exists. When a Windows program tries to execute code that doesn't exist, an error is generated. This error terminates the Adobe Reader process.

```
%PDF-1.1

1 0 obj
<<
 /Type /Catalog
 /Outlines 2 0 R
 /Pages 3 0 R
>>
endobj

2 0 obj
<<
 /Type /Outlines
 /Count 0
>>
endobj

3 0 obj
<<
 /Type /Pages
 /Kids [4 0 R]
 /Count 1
>>
endobj

4 0 obj
<<
 /Type /Page
 /Parent 3 0 R
 /MediaBox [0 0 612 792]
 /Contents 5 0 R
 /Resources
 << /ProcSet 6 0 R
   /Font << /F1 7 0 R >>
 >>
>>
endobj

5 0 obj
<< /Length 48 >>
stream
BT
/F1 24 Tf
100 700 Td
(Hello World)Tj
ET
endstream
endobj

6 0 obj
[/PDF /Text]
endobj

7 0 obj
<<
 /Type /Font
 /Subtype /Type1
 /Name /F1
 /BaseFont /Helvetica
 /Encoding /MacRomanEncoding
>>
endobj

xref
0 8
0000000000 65535 f
0000000012 00000 n
0000000089 00000 n
0000000145 00000 n
0000000214 00000 n
0000000381 00000 n
0000000485 00000 n
0000000518 00000 n
trailer
<<
 /Size 8
 /Root 1 0 R
>>
startxref
642
%%EOF
```

Figure 1: Code for the PDF document "Hello World"

Passing program control to an arbitrary address in memory is the holy grail of malware authors and exploit writers. This is what they need to make applications vulnerable to execute their own code. Very skilled exploit writers can achieve total control of the address to which execution jumps. (This is called Extended Instruction Pointer—EIP—control; EIP is the CPU's instruction pointer—that is, the register that points to the address in memory that contains executable code.) Exploit writers first place their own code at this address, then exploit the vulnerability so that program execution passes to this address.

However, it's rare to find such exploits with total EIP control in malicious PDF documents in the wild. (Malware found "in the wild" is malware that's spreading unrestricted on the Internet—not including proof-of-concept malware that isn't spreading, or malware used in very targeted attacks.) What's often found in the wild is PDF malware with exploits that achieve partial EIP control. Malware authors can build an exploit to jump to a particular address in memory, outside the normal program execution, but they can't build an exploit to jump to an arbitrary address in memory. They use a heap spray technique in JavaScript to plant their malicious code in memory: They fill the vulnerable program's dynamic memory (the heap) with malicious shellcode. Shellcode is a small program written in machine language that can execute correctly anywhere in memory.

Shellcode used in common malicious PDF documents is very small and typically does the following: It downloads an executable file from a web server on the Internet with an HTTP request, writes this file to the disk in the system32 folder, and executes the downloaded file. The shellcode has no real malicious payload; it's simply a downloader program that downloads and executes the real Trojan from the Internet. (Downloading a Trojan from the Internet provides malware authors with more flexibility; they can change the Trojan on the web server after they release their malicious PDF document in the wild.) This Trojan is what ultimately infects your machine—for example, by making it a member of a botnet.

In summary, here's how a typical malicious PDF document performs its nefarious actions. When the document is viewed with a PDF reader, a JavaScript script automatically executes. This script fills the heap with shellcode and then triggers a bug (in the PDF language or in the JavaScript language). This action leads to the execution of the shellcode and finally to the download and execution of a Trojan.

Mitigation Techniques

What can IT professionals do to prevent malware authors from exploiting bugs? One solution that PDF software vendors often recommend is to disable JavaScript. This action is useful for newly discovered vulnerabilities because it prevents the heap spray from executing.

Another good mitigation technique is to use Least-Privileged User Accounts. Because shellcode in many malicious PDF documents writes Trojans to the system32 folder, it requires administrative access. Removing administrative access prevents the downloader shellcode from operating. It can download the Trojan, but it can't write the Trojan to the system32 folder and therefore can't execute the Trojan. Furthermore, many Trojans require administrative rights to insert themselves into the OS.

Data execution prevention (DEP) is another important mitigation technique. In Windows, memory is marked as data or as executable. The heap is actually data—it's not meant to contain executable machine code. But until the introduction of DEP in Windows XP SP2, microprocessors executed instructions stored in memory designated as data without any problem. DEP changes this behavior of the microprocessor: It no longer executes code (including shellcode) stored in data memory (such as the heap).

To prevent exploitation of bugs, PDF reader vendors must designate memory, such as the heap, as data and activate DEP for their programs. If vendors fail to do so, administrators can still use the Microsoft Enhanced Mitigation Experience Toolkit (EMET) to force DEP on specific programs.

However, exploit researchers have found ways around DEP. Instead of writing their custom shellcode to the heap, they build custom code by borrowing existing instructions from code that's already loaded into the process address space via executable files (.exe and .dll files). This technique is called return-oriented programming (ROP), and the parcels of borrowed code are called ROP-gadgets. When skilled malware authors can predict where the executable files are loaded into memory, they can borrow code from these executable files for their ROP-gadgets and thereby exploit vulnerabilities in DEP-protected applications. To address this issue, Windows Vista introduced Address Space Layout Randomization. ASLR ensures that executable files are loaded at a (semi-) random address in memory, which prevents malware authors from predicting where their ROP-gadgets will be found in memory.

To benefit from ASLR, you must use a recent Windows version that supports ASLR (XP doesn't). In addition, the application authors must have marked the executable files for ASLR support. If a software vendor

doesn't include ASLR support in an application, you can still use EMET to force it.

Even software applications that do support ASLR can become vulnerable to ROP attacks when they include DLLs that don't support ASLR. For example, this is the case with some shell-extension DLLs. Shell extensions provide extra functionality to Windows (e.g., in the right-click Windows Explorer context menu). When you install an application such as WinZip, the setup program also installs a shell extension that provides WinZip integration with the right-click context menu in Windows Explorer, as well as all other applications that use the open and save common dialog boxes. Fortunately, WinZip's shell-extension DLL supports ASLR, so it doesn't expose the hosting applications to ROP attacks. But not all software providers are as security minded as WinZip; some software providers install shell-extension DLLs that don't support ASLR—and these DLLs expose hosting applications to ROP attacks. Applications such as Windows Explorer and Adobe Reader host shell-extension DLLS.

Another mitigation technique that's becoming popular is sandboxing. With sandboxing, the vulnerable application is more or less isolated from the resources of the underlying OS. As an administrator, you can use special sandboxing applications to isolate your vulnerable applications. In addition, vendors are starting to include sandboxing in their own products (e.g., Internet Explorer—IE—7.0, Microsoft Office 2010, Adobe Reader X). Sandboxing relies on Windows security features, such as integrity levels and restricted tokens, to contain exploits and malware inside the sandbox. Running inside the sandbox, the attacking shellcode is restricted. Depending on the type of sandbox, it has read-only access to the file system and registry (e.g., Adobe Reader X) or is completely isolated (e.g., Google Chrome).

Multi-Layered Protection

The best solution for mitigating PDF vulnerabilities is to use the most recent applications and OSs. If your application vendors fall short, you should implement mitigating actions yourself with EMET and sandboxing software. Although I focus on PDFs and Adobe Reader in this article, the solutions I present apply to all types of applications that produce and manage documents, including Microsoft Office.

Note that this article focuses on mitigation of malware found in the wild. Mitigation of highly targeted attacks can be much more difficult, depending on your opponent. In this type of attack, your opponent knows your environment and tailors the malware to operate successfully in that environment without detection. If you're a financially interesting target and your opponent is skilled and resourced, you'll need to go beyond the measures that I describe here—such as implementing application whitelisting.

InstantDoc ID 139862

Didier Stevens
(didier.stevens@gmail.com) works for Contraste Europe NV. He's a Microsoft Consumer Security MVP and a leading expert on malicious PDF files. You can find his open-source tools on his blog at blog.didierstevens.com.

FEATURE

SharePoint 2010 Goes Social, Part 2

Populating the User Profile via synchronization

by Kevin Laahs

In the first part of this three-part series on SharePoint social computing features, I discussed how the User Profile plays a key role in delivering the overall social networking experience. (See "SharePoint 2010 Goes Social, Part 1," June 2011, InstantDoc ID 129949.) This month, I discuss how to populate the User Profile via synchronization with other directory sources—specifically with Active Directory Domain Services (AD DS). Part 3 will describe the primary features that are used to better exploit a major information asset of any organization: its people. Note that the social networking features described in this article are available only in a SharePoint Server 2010 deployment and not in a SharePoint Foundation 2010–only deployment.

Understanding Profile Synchronization

Many organizations have several locations that store user information, from HR databases to enterprise directories. Some locations are application-specific, whereas others are multipurpose. Active Directory (AD) is an example of the latter. It's used as an authentication store as well as a directory store for applications such as Microsoft Exchange Server. Given the need for multiple locations, most organizations use a centralized enterprise directory as a master directory, and they use this directory to synchronize content with other stores, as required.

The User Profile store introduces yet another location that stores information about people. So, you may have to populate certain properties in your User Profile store from one or more repositories. Because it's important to keep user information consistent across all repositories, you must consider whether to grant users the right to modify such properties. This decision affects how such properties are synchronized with external sources.

SharePoint Server 2010 Profile Synchronization lets you integrate user and group information with the User Profile store when that information is coming from external LDAP directory services (such as AD DS) or from business systems that have been defined via the Business Data Connectivity service (such as SAP or Siebel). You integrate this information by defining connections to the external systems and by mapping individual user profile properties to appropriate properties in the external source.

Furthermore, you can indicate whether each mapped user property is to be synchronized for import or export (but note that mappings to business systems do not support the export capability). When you couple this ability to map a property for export with the option of allowing users to edit user profile properties, you get a powerful result where the value of this property in the external service directory is concerned: These twin features let you put the maintenance of this property value into the hands of your users. However, given the importance of maintaining consistency, you may not consider this appropriate for your own situation.

Microsoft Forefront Identity Manager is the actual engine that's used to execute and control synchronization between the various directory sources. It acts as the central metadirectory for all directory

services that are involved in synchronization. This component isn't enabled by default, but it's installed as part of the overall configuration of Profile Synchronization.

Configuring Profile Synchronization with AD DS

Before you tackle the various high-level tasks that are required to set up synchronization with AD DS, it's important to note that Profile Synchronization is not supported on a standalone installation but only on a server farm installation. (For development and testing purposes, a server farm can be a single server that's running all roles.)

The main tasks to perform during synchronization are as follows:

- starting the User Profile Synchronization Service
- defining your AD connections
- defining properties to be mapped
- invoking and monitoring synchronization

To run the process, you will have to know the name of your farm account. This is the name that you supplied when you ran the SharePoint Configuration Wizard after you installed SharePoint. This account is the one that you'll use to access the configuration database, and it's also the account that serves as the identity for the SharePoint Central Administration application pool in Microsoft IIS. If you forget your farm account name, you can retrieve it from IIS.

Starting the User Profile Synchronization Service

The User Profile Synchronization Service is the service that does the main lifting as far as synchronization is concerned. It leverages the Forefront Identity Manager services, which are not enabled by default.

The first time you start the User Profile Synchronization Service, you are effectively completing an installation of the required Forefront Identity Manager services. Do not be alarmed if this step takes a significant amount of time. The Forefront Identity Manager services run under the farm account, and these services must meet several prerequisites before the account can fully participate in the synchronization process. Therefore, before you start the User Profile Synchronization Service for the first time, you can help the process along by verifying that the following conditions are true:

- Your farm account is a member of the local Administrators group on the SharePoint server on which the User Profile Synchronization Service will run.
- Your farm account can log on locally to the same SharePoint server.
- If you're using a Windows Server 2003 AD forest, the farm account is a member of the Pre-Windows 2000 Compatible Access group for the domain with which you're synchronizing.
- You have a User Profile Service application running in your farm. This is typically handled during the post-installation process via the Farm Configuration Wizard, but it can also be configured through Central Administration. To do this, click the New button on the Manage Service Applications page, which you open from the Application Management page.

The first prerequisite affects only the initial provisioning of the Forefront Identity Manager software. Therefore, you can remove the farm account from the local Administrators group when everything is running smoothly. Note, though, that some community evidence suggests that doing this breaks subsequent synchronization. Therefore, if you experience issues after you remove the farm account, try troubleshooting by re-adding the account. The reason for this prerequisite is to make sure that correct encryption keys can be generated for the Forefront services during the initial provisioning. If you don't add the farm account to the local Administrators group before you provision the synchronization service, you must first reset everything before you try to reprovision the service. To do this, reboot your server, and stop the User Profile Synchronization Service by using Windows PowerShell. To stop the service, determine its GUID by using the Get-SPServiceInstance cmdlet, then pass this GUID into a Stop-SPServiceInstance cmdlet.

After you verify that the farm account meets the prerequisites, you can proceed to start the User Profile Synchronization Service by clicking the *Manage Services on server* link in the System Settings section of Central Administration. Make sure that the selected server indicated at the top of the page is the one on which your User Profile service application is running, and associate this server with your User Profile Synchronization Service. After you do this, the status of the service changes to Starting. You must now be patient while the Forefront Identity Manager services and the necessary connections to relevant SQL Server databases are configured. This step can take up to 15 minutes. A successful conclusion to this step is indicated by a change in the status of the service from Starting to Started. Note that if Central Administration is running on the same server, you must reset IIS after the service is started.

There are some things you can check to verify that the configuration is complete. For one, the Forefront Identity Manager and Forefront Identity Manager Synchronization Windows services should be running. Also, these services should be associated with your farm account and have a startup type of Automatic. (You should not start these services manually. They must be started by using the User Profile Synchronization Service.) Finally, make sure that the %Programfiles%\Microsoft Office Servers\14.0\Synchronization Service\MaData folder has been created and that several empty folders have been created within it.

Defining Connections to Active Directory

Profile Synchronization lets you use AD as a master source for populating the SharePoint User Profile. This means that as user and group objects are created, updated, and deleted in AD, they are also created, updated, and deleted in the SharePoint User Profile.

To indicate those objects in AD that you want to synchronize, you create a Synchronization Connection item. During creation, you define the type of directory service that the connection relates to, as well as the objects within the directory that should be synchronized. The following factors affect this process.

Knowledge about your AD forests is required. You must be familiar with such aspects of your AD installation as forests, domain controllers, and organizational units so that you can point your connection at those containers that hold the user and group objects that you want to synchronize

with. You must also know whether any of the default port numbers for LDAP access have been changed and whether you are required to use an encrypted LDAP connection (i.e., whether SSL is required).

Filtering of objects may be required. You can specify a filter to the connection and use the filter to fine-tune the objects and groups that you want to pull from AD into the User Profile. If your organization leverages an AD property as part of a provisioning process to determine which users you want to include in the SharePoint User Profile, you have to know which properties are used and what their values should be.

Resource forests are supported. Support is provided if you have two AD forests—one that's used for authentication (i.e., the forest that users log on to, commonly known as the account forest or logon forest) and one that's used for resources (such as Exchange or SharePoint). In this case, the objects in the resource forest are appropriately secured so that they can be used by users who log on to the account forest. Entries in the User Profile are linked to their counterparts in AD by way of the user's SID, which is associated with the user's account forest object. Therefore, in a resource forest scenario, you should link the objects by using the account forest, but you should obtain most of the attributes that require synchronizing from the resource forest. To follow this scheme, you must set up two connections—one for the account forest and one for the resource forest. The User Profile then contains the SID for the object in the logon forest and the SID from the associated object in the resource forest.

Appropriate account permissions are required. You must use an account that has the appropriate permissions for the actual synchronization. This account will be designated as the service account for the Metadirectory Services Active Directory Management agent (i.e., Forefront Identity Manager). This account must meet the following requirements to have the appropriate permissions:

- The account must have Domain Administrative permissions, it must belong to the Domain Administrators group, or it must be explicitly granted Replicating Directory Changes permissions for every domain in the forest that this management agent accesses. You can use an ACL editor or ADSI Edit to add an access control entry to the domain object that grants your account the Replicating Directory Changes permission.
- If the NETBIOS name is different from the domain name, the cn=configuration container must have at least the Replicating Directory Changes permission. Refer to the Get-SPServiceAppliction cmdlet topic in PowerShell Help for more information about how to enable NETBIOS names on a User Profile Service application.
- The account must be a member of the Farm Administrators group, or the account must be designated as a User Profile Service administrator.
- If you intend to export user properties from SharePoint into AD DS, the account must have the Replicating Directory Changes permission on the object and on all child objects for the AD DS domains to which you want to export data. If you intend to export the picture property, the read/write permission is also required on the container that stores the attribute, which is the container to which you want to export. For example, the read/write permission is required on the container that stores the ThumbnailPhoto attribute for profile pictures.

When you have the required information in hand, you can use Central Administration to create a connection to AD by selecting the Configure Synchronization Connections option in the Synchronization section of the User Profile Service Application page.

After you click Populate in the Containers section of the User Profile Service Application page, you will be able to navigate through your AD installation and select the containers that contain the objects you require. To make the selection, select the check box next to the container name. You must select at least one container. Note that selecting a container automatically selects all the objects contained in it. Note, too, that although you can select individual objects at this stage, a more common approach would be to select the highest-level container in which your desired objects reside, and to use a filter to extract only the relevant objects from those containers. You can see an example of a successful connection in Figure 1, with the Users container selected.

To fine-tune the objects that are imported, you can define exclusion filters on the Manage Connections page. To do this, hover the mouse pointer over your connection to display a context menu, and click Edit Connection Filter. On the next page, you can specify exclusion filters for both user and group objects. You can see this in Figure 2, where I have indicated that objects should be excluded if their extensionsAttribute1 value is not equal to 1. The other filter that you see in Figure 2 excludes disabled objects. This is because of the value setting of the AD DS attribute userAccountControl. The second bit of this value is set if an account is disabled.

Defining Properties to be Mapped

You now have to decide which user profile properties to map to AD, and you must also decide how to direct the mapping for each property. A property can either be imported or exported. In an import process, the AD attribute value is written into the mapped user profile property. In an export process,

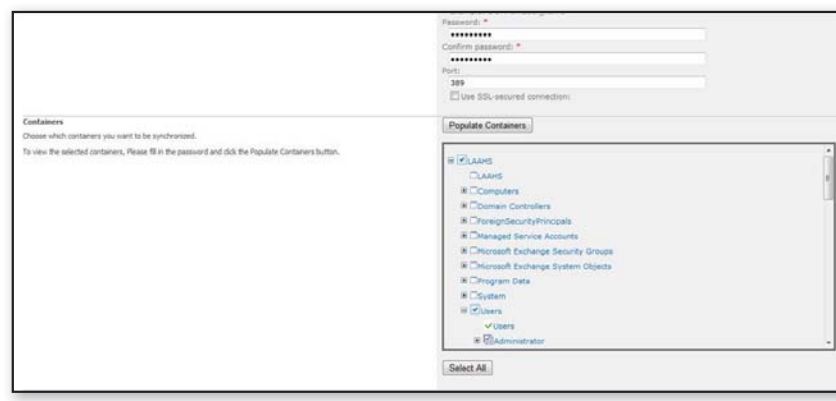


Figure 1: Browsing containers

Figure 2: Setting exclusion filters

the user profile property is written into the mapped AD attribute.

You have out-of-the-box access to a default set of mappings for an AD connection, as shown in Table 1. Note that all default properties are marked as Import. You can override most of these mappings to suit your needs, and you can add new mappings for the properties that you have defined in your own User Profile. For example, you can update an AD extension attribute for a custom property that users are permitted to edit through their own profiles. This custom property could then be available to other applications that use that AD installation. To define such mappings, click the Manage User Properties link on the User Profile Service Application page, and select the Edit option.

Table 1: Default mappings

AD DS attribute	User Profile property
objectSID	SID
<logon id e.g. {domain}/{user}>	ADGuid
givenName	FirstName
msDS-PhoneticFirstName	PhoneticFirstName
Sn	LastName
msDS-PhoneticLastName	PhoneticLastName
displayName	Name
msDS-PhoneticDisplayName	PhoneticDisplayName
telephoneNumber	WorkPhone
Department	Department
Title	SPS-JobTitle
Manager	Manager
sAMAccountName	UserName
wWWHomePage	PublicSiteRedirect
proxyAddresses	SPS-SipAddress
Dn	SPS-DistinguishedName
msDS-SourceObjectDN	SPS-SourceObjectDN
Mail	WorkEmail
physicalDeliveryOfficeName	Office

Invoking and Monitoring Synchronization

The synchronization process involves many stages, and it can take a long time to finish. The process must detect changes in both directory sources. It must also determine which changes apply to which objects (i.e., which attributes must be written from AD to the user profile and which must be written from the user profile to AD). Finally, the metadirectory service must process the changes, which can involve updates, additions, and deletions.

There are two modes in which you can execute synchronization: full and incremental. A full synchronization is required only if you want to perform a full reset of the User Profile. An incremental synchronization is the preferred method because it processes only those objects that have changed in either directory source since the last synchronization was performed. During synchronization, any new AD objects that are found in the mapped containers and that are not excluded by any filter rules are added to the User Profile. These objects are added with the required attributes mapped. The metadirectory uses the objectSID attribute to link the AD user object and the User Profile. This attribute is used to locate existing User Profiles for AD objects that have been modified or deleted.

Synchronization can be invoked manually, and you can also set up a schedule for an incremental synchronization to run at a time of your choosing. Because synchronization is resource-intensive, consider running the process outside your core working hours.

You execute synchronization by using the Start Profile Synchronization option on the User Profile Service Application page. While the process is running, you can monitor its status in the Profile Synchronization Settings section on the right side of the screen. This section also provides you controls to stop the synchronization process and to view its progress. The number of stages in the process is dependent on the number and type of connections you have configured. The progress of each stage is displayed on the page that's produced when you select the Synchronization option.

After synchronization is complete, you can view the User Profiles by using the Manage User Profiles option. Note, however, that nothing is displayed! This is the default view setting. To see profiles, you must enter a filter string and click the Filter button to display entries that match the string. A good way to list all entries is to enter the domain name of your AD objects as the string. This is because all your User Profile entries will have the domain name in the Account Name User Property value.

Aiming Toward Connection

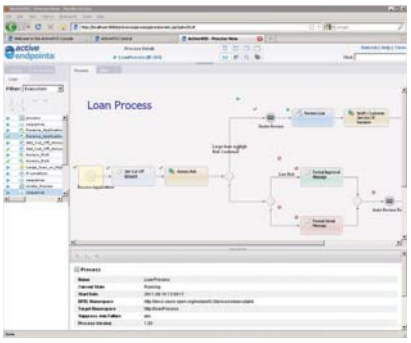
Maintaining rich, up-to-date information in your User Profile facilitates better use of an important resource: your people. Synchronizing with repositories such as AD is the best way to make sure this information is consistent across your organization. In part three of this article, we'll see how to use the information contained in the User Profile to connect people through social networking features.

InstantDoc ID 136368

Kevin Laahs
(kevin.laahs@hp.com) is a technology strategist with HP Enterprise Services. Kevin is coauthor of four books about SharePoint, the latest of which is *Microsoft SharePoint 2010 All-in-One For Dummies* (Wiley).

Active Endpoints Announces ActiveVOS 9.0

Active Endpoints has announced the availability of **ActiveVOS 9.0 Enterprise Edition** and a new **Data Center Edition.** These latest releases deliver a scalable and secure SOA-based business process management system that supports multi-tenant



virtual partitioning and resource sharing, multi-site clustering for large IT organizations to deploy private clouds, and enables Software as a Service (SaaS) providers to deploy more cost-effective public clouds. Additional features of ActiveVOS 9.0 Enterprise and Data Center Edition include an enhanced process designer and a new performance dashboard. The new release also includes improved standards support that is fully compliant with BPMN 2.0, XQuery 3.0, and XSLT 2.0 standards. To learn more, visit www.activevos.com.

Siemon Offers Flat-Cable Category 6 Compatible Patch Cords

Siemon announced the release of new **category 6 compatible flat patch cords** for in-cabinet network equipment

connectivity. These RJ45 copper cable assemblies support category 6 transmission performance in a low-profile construction that provides tighter bend radius and easily managed cable routing. These patch cords use four pairs of 28-gauge cable in a rectangular cross section that is only 2.2mm thick. The small profile lets two to three flat cables be neatly bundled in the space of a single round 24-gauge cable. To learn more, visit www.siemon.com.

Egnyte Releases Personal Local Cloud 6.0

Egnyte has released **Personal Local Cloud 6.0** and the **Egnyte Outlook** email plug-in. These tools let users easily browse and share files in the cloud directly from their desktops or within Microsoft Outlook. Egnyte's Personal Local Cloud includes a visual sync indicator on each file and folder that lets users confirm that each file is up-to-date. In addition, Egnyte's Personal Local Cloud has the ability to share files by generating links directly from the desktop, and it provides seamless enforcement of all business policies set by the company administrator. To learn more, visit www.egnyte.com.

Recover Lost and Forgotten Passwords

Passcape Software has released **Passcape Windows Password Recovery 2.0,** an application that lets users regain access to Windows, even if passwords have been lost or forgotten. Passcape Windows Password Recovery uses password recovery algorithms, artificial intelligence, and comprehensive dictionaries of passwords and pass-phrases to identify and unlock Windows. The program supports 11 different types of password recovery techniques. These methods are supported by 2GB of

PRODUCT SPOTLIGHT

Lenovo Updates ThinkServer Family for Small Businesses

Lenovo announced **TS130** and **TS430** to its ThinkServer family. The new additions feature the latest Intel Xeon process technology and remote management tools. The TS130 and TS140 give small-to-midsized businesses and corporate branch offices a performance boost and business tools.

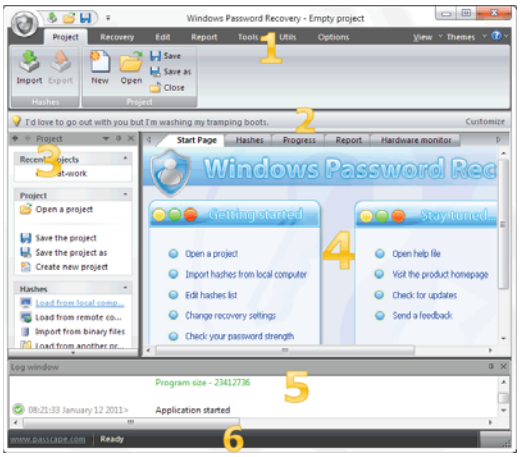
"The Lenovo ThinkServer TS130 delivers capabilities that small business owners need in a server by including

features like the latest Intel Active Management Technology—an outstanding remote manageability solution," said Boyd Davis, vice president and general manager of Data Center Group Marketing at Intel.

The single-processor TS130 and TS430 leverage the Intel Xeon E3-1200 processors, which offer up to 30 percent better performance than previous generations. Equipped with Intel's AMT 7.0 manageability tools, the ThinkServer TS130 comes with enterprise class storage choices, onboard RAID, and remote manageability features. The ThinkServer TS430 offers 16TB of hot swap storage capability, SAS RAID data protection, and redundant power choices. In addition, the TS430 offers front-side drive access and a ThinkServer Management Module with available iKVM.

"The ThinkServer TS430 changes the game for small business servers," said Tom Ribble, director of worldwide marketing for Lenovo's ThinkServer Business Unit. "With outstanding storage scalability, premium SAS RAID, and redundant power choices, the ThinkServer TS430 delivers all these features and world-class quality at unmatched prices."

Pricing for TS130 begins at $657, and TS430 begins at $699. To learn more, visit www.lenovo.com.



organizations secure networks and achieve regulatory compliance. TrustNet Manager's drag-and-drop security policy builder simplifies provisioning and lets users deploy multilayer encryption and security policies. In addition, TrustNet Manager provides role-based access to multiple users, giving teams control of encryption keys and network security policies. TrustNet Manager is based on a clustered server architecture with disaster recovery capabilities and is able to generate and deliver periodic key updates. To learn more, visit www.certesnetworks.com.

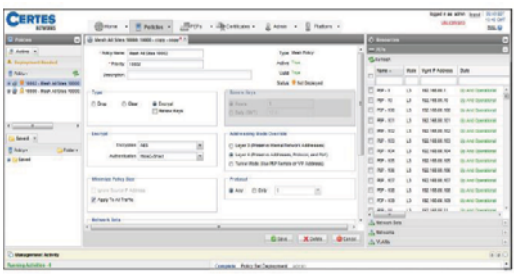
dictionary data, which is available online from within the program, and work with ASCII, Unicode, UTF8, and PCD formats. To learn more, visit www.passcape.com.

Netuitive Releases Netuitive 5.5 for the Enterprise

Netuitive announced the latest release of its predictive analytics software, **Netuitive 5.5.** Built for large enterprises, Netuitive 5.5 is a performance management platform for mission-critical applications running in physical, virtual, and cloud infrastructures. The new release resolves IT issues before they impact quality of service. New product features help IT organizations eliminate virtual server sprawl, optimize server consolidation ratios, enable long-term capacity trending, and improve the manageability of virtualized applications. Additional features in Netuitive 5.5 include a flexible one-view dashboard, chargeback reports, and support for multi-hypervisor environments. To learn more, visit www.netuitive.com.

Secure Networks with TrustNet Manager

Certes Networks announced the general availability of **TrustNet Manager,** a web-based management platform that lets



Vormetric Announces Transparent Encryption for SAP

Vormetric announced **Vormetric Data Security for SAP,** a solution that protects data in SAP environments with transparent encryption. The solution provides centralized, secure key management and separation of duties. In addition, Vormetric's solution requires no changes to SAP and protects information both inside and outside of databases. The solution has the ability to protect both structured and unstructured data, including SAP reports, archives, and database extracts. Vormetric supports databases including IBM DB2, Microsoft SQL Server, Oracle, and Informix. To learn more, visit www.vormetric.com.

Rectiphy Releases ActiveImage Protector for Hyper-V

Rectiphy has released **ActiveImage Protector for Hyper-V with ReZoom 3.0,** which includes enhancements to its live data, sector based, backup, and restore solutions for Microsoft's virtual environment. ActiveImage Protector adds new features, including speed enhancements, resource usage adjustment options, and the ability to combine incremental and full backup images for long-term data storage. This release supports the next generation of UEFI motherboards and GUID partition tables. To learn more, visit www.rectiphy.com.

Paul's Picks

www.winsupersite.com

SUMMARIES of in-depth product reviews on Paul Thurrott's SuperSite for Windows

Windows 8 Start Screen

PROS: A single UI that works well across devices (PCs, phones, Xbox) and user scenarios (home, work, server)

CONS: Such a dramatic UI change requires retraining

RATING: ◆◆◆◆◆

RECOMMENDATION: Microsoft has been planning for quite some time now to bring a new, cohesive user experience to virtually every end-user product it makes: phones and tablets, of course, but also notebook and desktop PCs, the living room, and, I think (or at least hope), the server. Our first peek at this user experience was the Windows Phone OS "Metro" UI, but now that we've seen this UI implemented in the Windows 8 Start screen as well, it's starting to all come together. What's amazing is that Microsoft was able to create a single UI that works well on phones, ARM-based slate, x86/x64-based slate, and convertible tablets, netbooks, notebooks, Ultrabooks, PC desktops, the Xbox 360 and, perhaps, media center PCs (and, I hope, the server). This single UI can be controlled with touch and multitouch, with keyboard and mouse, with a remote control or Xbox 360 hand controller, or with voice or Kinect-based hand gestures in the air. And it works.

CONTACT: Microsoft • www.microsoft.com

DISCUSSION: bit.ly/m1VKdH

Windows Phone Mango Preview

PROS: Free; fills in many functional gaps in the initial release; deep integration with online services

CONS: Still no way for developers to integrate their services into Windows Phone hubs

RATING: ◆◆◆◆◇

RECOMMENDATION: Microsoft will provide Windows Phone Mango as a free update to all existing Windows Phone 7 handsets, so there's some value in that. Mango improves the platform's capabilities while using the same basic user experience, so the upgrade will be seamless and painless from a user perspective. Although Mango doesn't address some of the version 1 shortcomings, it adds so many useful features and fixes so many of the early complaints that I find it hard to criticize this release with any enthusiasm. I'll keep using it and report back when we get closer to the final release—but Mango looks great so far.

CONTACT: Microsoft • www.microsoft.com

DISCUSSION: bit.ly/jhLMnw

InstantDoc ID 139894

REVIEW

Specops Deploy

Desktop management, especially software and OS deployment, can be one of an IT administrator's most tedious tasks. Specops Software's Specops Deploy integrates with Active Directory (AD) and uses your organizational unit (OU) structure to target computers for application and OS deployments. Specops Deploy comes as three separate components: Specops Deploy /Application installs applications to Windows computers within AD; Specops Deploy /OS installs or re-installs OSs to bare-metal or existing computers; and Specops Deploy /Log Viewer consolidates and monitors log files.

To perform any of the available installations, you should use the Specops Setup Assistant. Although the assistant makes installation fairly straightforward, you must also install several software components for the product to run correctly. Run the Specopssoft.SetupAssistant file to launch the assistant. All the necessary setup files are included in this self-extracting executable file. As Figure 1 shows, the setup assistant verifies all installation requirements prior to installation.

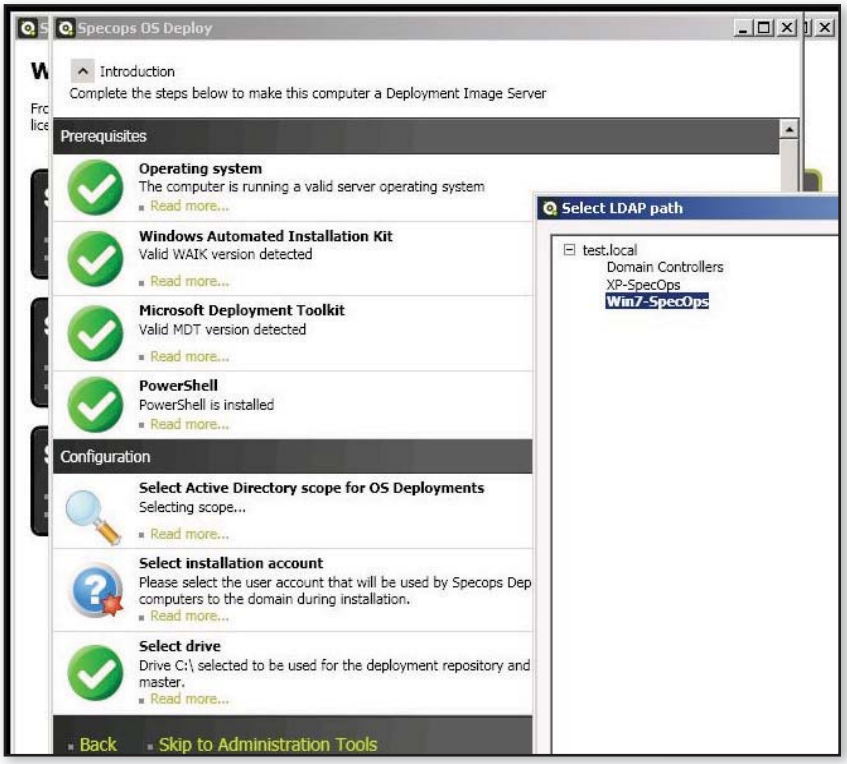


Figure 1: Using the setup assistant to verify installation requirements

Software Deployment

Before installing Specops Deploy /Application, you need to install the following:

- Microsoft SQL Server (I used SQL Server 2008 Express)
- .NET Framework 3.5 SP1 or later
- Windows Server 2008 R2, Server 2008, or Windows Server 2003 R2
- Group Policy Management Console (GPMC)—for Server 2008, you can add GPMC from Server Manager; for Server 2003, you can download GPMC from www.microsoft.com/download/en/details.aspx?id=21895

These components can be installed on multiple servers, although I used a single server in my lab environment.

After the Specops Deploy /Application installation is finished, open the Specops Deploy /Application software and select the *Install a new Deployment Server* option from the Server Configuration section. If you open GPMC, you'll see a new section in Group Policy, at [Computer Configuration]/[Policy]/[Software Settings]/[Specops Deploy /Application]. Specops Software recommends that you create a new OU within AD and link a new Group Policy Object (GPO) to this OU. When working within the Specops Deploy /Application console, the vendor recommends that you keep things simple by starting with a new GPO rather than mixing settings with an existing GPO. Specops Deploy /Application updates the selected GPO as you create and deploy software packages.

After the server setup was complete, I installed the client extensions on a Windows XP machine. The client extensions are provided in the form of an MSI file, so you should be able to install the extensions to a large number of desktops using only an AD GPO. After the client extensions were installed, I used Specops Deploy /Application to install additional MSI files. These installations repeatedly failed. Fortunately, the software includes a feedback mechanism that alerted me that access was denied to the deployment share. I promptly gave full control access to everyone for the share and NTFS—but the software still failed to install and still generated an access denied error. At this point, I went back to the documentation to verify that my installation was correct. Then I checked the Specops online documentation and forums, but I didn't find a resolution. I decided to try changing my installation share to a NAS device. This proved to be a successful workaround, and the MSI installation files installed without any problems. I later contacted a Specops representative, who told me that a conflict occurs when everything is installed on the same server, which can cause this permissions error.

Specops Deploy /Application refers to installation files with .exe extensions as a legacy installation—which is what I chose to test next. Within minutes, I was able to configure a deployment for CCleaner, Java,

Nate McAlmond | mcalmond@gmail.com

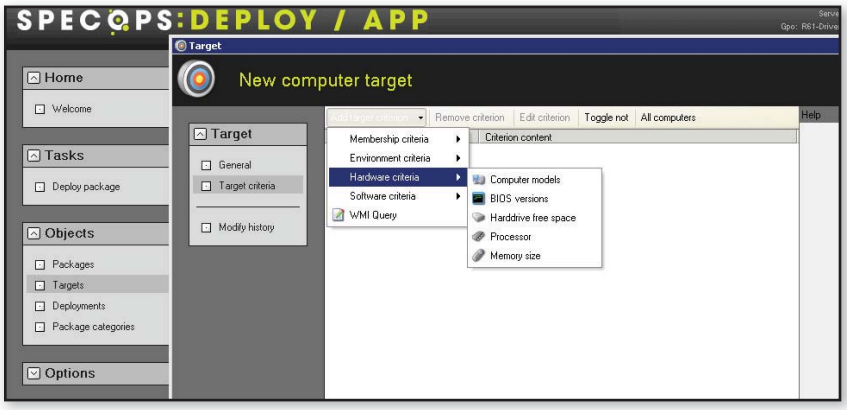


Figure 2: Application packaging wizard

and Defraggler. To install these types of packages, you must add the installation parameter for an unattended installation—which you can typically find with a quick online search. The unattended installation parameter for CCleaner and Defraggler is /S; the Java parameter is /s IEXPLORE=1 MOZILLA=1. I found the option to add these installation parameters in the Specops Deploy /Application UI. After I added the parameters, all three applications installed without any problems.

In addition to installation parameters, Specops Deploy /Application includes several other options that you can add, such as:

- Pre-install commands and parameters
- Post-install commands and parameters
- Pre-uninstall commands and parameters
- Post-uninstall commands and parameters

These options are available in the UI's advanced sections.

Specops Deploy /Application also includes a section where you can specify which computers will receive your deployment package, as Figure 2 shows. This option simplifies deployment by letting Specops Deploy /Application intelligently take into consideration such things as the amount of RAM, free disk space, processor type, OS, group membership, IP range, and Windows Management Instrumentation (WMI) query, to name a few. This option gives administrators the ability to move a large number of computer accounts into the OU and let Specops Deploy /Application decide which deployment packages are appropriate for which computers, without administrators having to continually micromanage the situation.

OS Deployment

The Specops Deploy /OS portion of the software suite runs only on Server 2008 R2 and Server 2008. I therefore prepared another server for this portion of my evaluation. Before installing the Specops Deploy /OS software, you need to install the following:

- Windows Automated Installation Kit (www.microsoft.com/download/en/details.aspx?id=9085)
- Microsoft Deployment Toolkit (www.microsoft.com/download/en/details.aspx?id=25175)

Specops Deploy integrates with Active Directory and uses your organizational unit structure to target computers for application and OS deployments.

- PowerShell (support.microsoft.com/kb/968929) or Windows Update
- Windows Deployment Services—which is a Server 2008 Server Manager role
- Group Policy Management—which is a Server 2008 Server Manager feature
- Enough hard drive space to store the OS images
- Target computers that support booting from the network (Preboot Execution Environment—PXE—boot)

Before deploying an OS, you need to load the base image from media, which I did from an XP CD-ROM. After the base OS image is loaded into Specops Deploy /OS, you can capture an image from one of your AD-connected computers by selecting *Load image from existing computer*. This option adds a file called SpecopsImage Capture.cmd to the root of the C drive on the target computer that you previously selected. When you double-click Specops ImageCapture.cmd, the target computer is prepared for duplication with Sysprep, and the necessary files are then copied to the Specops Deploy /OS server. However, you must first make sure that the target computer is accessible from the Specops Deploy /OS server via WMI and that it allows blank passwords. The easiest way to accomplish this is to temporarily turn off the Windows firewall (thus allowing WMI connections), alter the local Group Policy settings to allow passwords of zero length, and disable password complexity.

In addition to images, you can specify which language packs and drivers are included with your OS installations. Drivers can be loaded from the file directory or imported from an existing computer on your network from the Specops Deploy /OS software.

Before you begin deploying OSs, you should look at the Specops Deploy /OS software's policy section. You can change the default policy, which is used every time you deploy an OS with Specops Deploy /OS unless you specify a custom policy from the Group Management console—which you can launch from the Specops Deploy /OS software's Policy section. Custom policies are added by configuring a GPO in the [Computer Configuration]/[Policy]/[Software Settings]/[Specops Deploy /OS] section and are applied to computers in their corresponding OUs. From the default policy or a custom policy, you can change installation settings, such as the local administrator password, OS settings (e.g., forcing an x86 image on all computers, which OS to install on x86 and which OS to install on x64 computers), and migration of user state and location settings (e.g.,

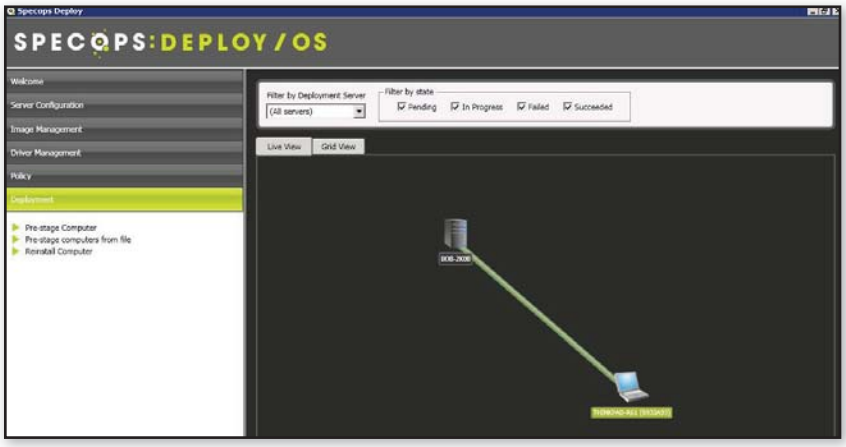


Figure 3: OS deployment status

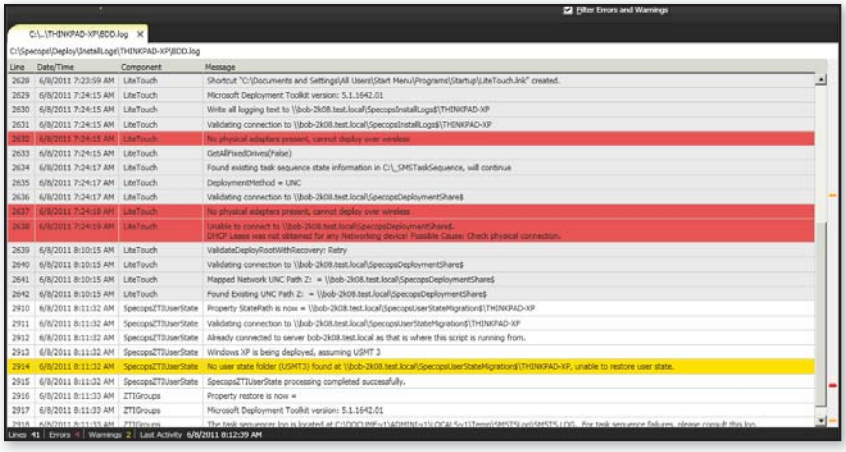


Figure 4: Log Viewer review of OS deployment

what time zone and language to use when deploying an OS).

To start an OS installation with Specops Deploy /OS, you need to first stage the machine in the Specops Deploy /OS software on the server. To do so, select the *Pre-stage Computer* or *Pre-stage computers from file* option. This action launches the Pre-stage Computer wizard, where you must specify the machine's GUID and where in AD the computer account should be located.

After you have the target computer pre-staged, you might need to verify that the boot order has the hard drive listed after the PXE boot. Then, start the target computer and let it PXE boot during the startup process, which initiates the OS installation. Specops Deploy /OS prepares the hard drive of the target machine by deleting the current hard drive partitions and creating one large partition of maximum size. Then, Specops Deploy /OS downloads all the necessary files to the target machine and reboots. After reboot, the target machine boots from the local hard drive and begins installing the previously downloaded OS installation files. You can watch the OS installation progress from the Specops Deploy /OS software's Deployment section, as Figure 3 shows.

I ran into a few problems with Specops Deploy /OS when targeting a virtual machine (VM). In Sun Microsystems's VirtualBox, the network driver failed to load during the unattended installation; in Microsoft Virtual PC 2007, the installation failed, with an error indicating that 16MHz isn't a supported processor speed. When I switched to a Lenovo ThinkPad laptop, the XP installation completed without any problems.

Log Monitoring

Specops Deploy /Log Viewer is also included with the Specops Deploy suite and is free to continue using even if you don't purchase Specops Deploy. Specops Deploy /Log Viewer makes it easier to review and monitor log files that are in the Microsoft Deployment Toolkit format. Using this tool gives administrators some obvious advantages over opening a log with Notepad, including the following:

- Errors and warnings can be filtered.
- Errors are indicated in red along the right-hand bar, making it easy to go directly to that section of the log.
- Log files are shown in real time, so you don't have to keep refreshing to see the new log entries.

You can find the Specops Deploy log files at C:\Specops\Deploy\InstallLogs, as Figure 4 shows.

AD Integration Makes for Easy Implementation

Specops Deploy is a great management tool that lets administrators and Help desk staff simplify major new deployments, as well as ongoing application and OS installations. The product's tight integration with AD lets companies customize Specops Deploy to their own needs and existing hierarchies. In addition, the software's AD integration makes Specops Deploy familiar to most administrators and therefore decreases the learning curve.

InstantDoc ID 139672

Specops Deploy

PROS: Simplifies software and OS installation; simple setup; provides useful feedback

CONS: OS deployment component adds to the price and is unnecessary for many organizations

RATING: ◆◆◆◆◆

PRICE: $3,840 for up to 100 clients, at $32 per workstation with 1 year of support; $27,840 for up to 1,000 clients, at $23 per workstation with 1 year of support; government and educational discounts available

RECOMMENDATION: Anyone who needs to install and maintain applications or OSs on a large number of computers, whether in a geographically distributed or centrally located environment, will benefit from installing Specops Deploy.

CONTACT: Specops Software • 877-773-2677 • www.specopssoft.com

AirMagnet WiFi Analyzer Pro

The addition of WiFi networks, sometimes known as wireless LANs (WLANs), in a corporate environment can introduce a whole new class of threats for network security. Rogue Access Points (APs) can be installed by employees fairly easily and, because of their relatively small size, can be tucked away in corners and eventually forgotten. However, easy installation often translates to low security, especially for those whose full-time job isn't security related. These rogue APs probably don't adhere to corporate network security policies and therefore can introduce vulnerabilities into otherwise reasonably well-protected networks. If you've ever wondered what's traveling over the WiFi airwaves around your office, wanted to ensure that your WiFi network was performing well, or needed to know if any rogue devices were lurking on your WiFi network, Fluke Networks's AirMagnet WiFi Analyzer Pro might be just the tool for you.

This management software requires at least one WiFi interface device from the vendor's approved list that isn't currently operating as a live WiFi device. This device is used as an observer of traffic in the WiFi spectrum. The device can be installed on a desktop station to observe the traffic from a fixed location, or it can be attached to a roving laptop computer to check the WiFi network at different locations throughout the building or campus. A license for each listening device is required for AirMagnet WiFi Analyzer Pro. Although the list of approved devices is currently somewhat limited, it might improve in time. I connected a USB WiFi device to my Windows 7 desktop system for testing.

AirMagnet has a handy dashboard view that shows signal strength for each of the WiFi channels in the 2.4GHz and 5GHz bands for 802.11a/b/g/n networks; a channel utilization graph; and charts showing "top talkers," SSIDs by utilization, active device type, and more. From the main screen, you can also get a comprehensive list of all devices or subset lists of just the APs, individual stations, and ad hoc networks.

For my tests, I used my organization's own 802.11g and 802.11n APs and devices; I was also able to show activity from other nearby WiFi networks. In addition, in the views for devices, APs, and stations, I was able to place alias names on known devices and classify others as rogue devices. This let me quickly identify known devices on my organization's networks, as well as ensure that rogue devices weren't attempting network access. AirMagnet WiFi Analyzer Pro not only shows the devices on the networks but also indicates which APs (by service set identifer—SSID) they're using.

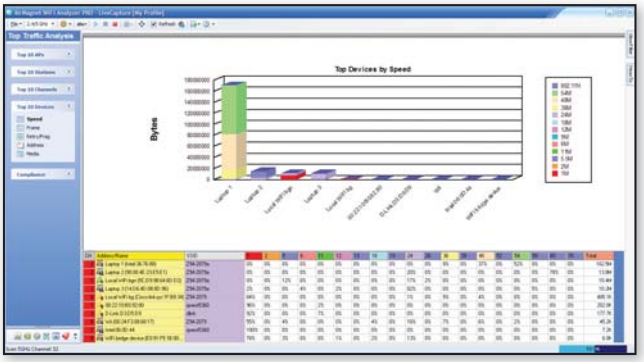


Figure 1: AirMagnet WiFi Analyzer Pro traffic analysis report

I like the device lists' color coding, which indicates how recently devices have been active: green for currently active (within the past 5 seconds), yellow for activity within 5 to 60 seconds, red for activity within 60 to 300 seconds, and gray for activity more than 300 seconds (5 minutes) old. You can sort the lists by any of the columns, which lets you check by time of activity, signal strength, SSID being accessed, and so on. You can also filter the views by several criteria, to help manage large networks.

AirMagnet provides signal-to-noise and signal-strength graphs for each WiFi channel. To show WiFi activity, I downloaded data from websites, created file shares between Windows 7 laptop computers, transferred files between systems over the air, and measured the results. You can perform traffic analysis by AP, top 10 stations, top 10 channels, and top 10 devices. You can further organize the results by various criteria. The report in Figure 1 shows the top 10 devices by speed. The chart shows the speed of data transfer, indicating how many bytes were transferred at which speed level.

The software also provides reports that show alarm conditions and compliance reports for various regulations. AirMagnet's alarm reports show activity that exceeds various thresholds. The compliance reports can help with HIPAA, Gramm-Leach-Bliley, Sarbanes-Oxley, Department of Defense (DoD) Directive 8100.2, FISMA, Basel II, ISO 27001 compliance, and more.

AirMagnet reports on dozens of security risks or potential risks, including devices not protected by encryption, rogue devices, and more. In my file-transfer tests, the software was able to detect the file transfers by noting the large number of Clear-to-Send (CTS) signals being transmitted.

Regardless of whether you're working in a large corporate environment or a small business environment, software for managing your WiFi networks is a good investment. AirMagnet WiFi Analyzer Pro helps you monitor your network traffic, ensure that the network is performing well, and alert you to any rogue devices.

InstantDoc ID 139859

AirMagnet WiFi Analyzer Pro

PROS: Comprehensive WiFi network information and management solution; includes information to help maintain regulatory compliance

CONS: Overwhelming feature set for those new to WiFi network management; short list of officially supported WiFi listening devices

RATING: ◆◆◆◆◇

PRICE: $3,995

RECOMMENDATION: AirMagnet is a good investment for businesses of any size that need to monitor and manage their WiFi networks.

CONTACT: Fluke Networks • 800-283-5853 • www.flukenetworks.com

Dennis Martin | dennis@demartek.com

One Admin. Countless Active Directory Responsibilities.

Quest Has Everything You Need for Your Compliance and Security Challenges

As an Active Directory Administrator, you're juggling several things at once. Management. Monitoring. Auditing. Procurement. Implementation. Quest solutions work seamlessly with all your diverse physical and virtual platforms, so no matter what the challenge, we've got a solution you can rely on.

See how Quest helps you with your Active Directory compliance challenges in "Overcoming Active Directory Audit Log Limitations" at *www.quest.com/OneAdmin*

Get the free mobile app at
http://gettag.mobi

QUEST SOFTWARE®
Simplicity At Work™

Active Directory Auditing Tools

Tools to track down security threats and prove regulatory compliance

by Eric B. Rux

The reality is simple: If you suspect that your network has been compromised, the built-in tools provided by Microsoft aren't going to be much help. Trying to find the culprit using Event Viewer is like looking for a needle in a haystack. You need a tool that can lay out the data in a clear and concise manner—you need a good Active Directory (AD) auditing tool. I'll show you six products that will bring a smile to your face and put your mind at ease.

My environment for testing each product consisted of a Windows Server 2008 AD domain hosted on a VMware ESXi host. I also added, when necessary, a separate server running Microsoft SQL Server 2008 or SQL Server 2008 Express to the domain. The products were installed on a domain controller (DC), SQL Server machine, or VMware virtual appliance. To create the organizational unit (OU) structure and add users to each domain, I ran a simple script that used the Dsadd command-line tool. Detailed side-by-side comparisons of each product can be viewed in Table 1.

Blackbird Group's Blackbird Auditor for Active Directory

Blackbird Group has a complete management suite for AD that consists of six modules, one of which is Blackbird Auditor for Active Directory. The modules can be purchased separately or together as a suite. All the modules are managed from the same management console. Unlike the other products in this review, Blackbird Auditor is licensed per employee, not by AD user, potentially saving you licensing costs.

Blackbird Auditor supports Windows 2000 AD and later. It should be installed on a dedicated server. It requires a Microsoft .NET Framework 3.5 and a SQL Server 2005 or later back end, which can be hosted on the dedicated server. However, SQL Server 2008 Express can be used for small environments (up to two DCs and a maximum of 2,500 users). For this review, I chose to use SQL Server 2008 Express.

After taking care of the prerequisites, you first install the Blackbird Management Suite Server software on the dedicated server. Licensing is handled with a .license file. The installation wizard walks you through setting up the Blackbird Service, directory connector, and back-end database. It also takes care of configuring the Windows Server firewall exceptions. Next, you install the console using the Blackbird Management Suite Console software. It can be installed on the dedicated server or on a Windows XP or later workstation. After the base application and console have been installed, one or more modules need to be installed. For this review, I installed only Blackbird Auditor.

Finally, you need to install an agent (what the company calls a handler) on each DC in your domain. This is done from the Management Suite Console by right-clicking the AD node and choosing *Deploy data handler.* The agent can be installed one DC at a time or on multiple DCs in a single operation.

Blackbird Auditor's main console is a Microsoft Management Console (MMC) snap-in. From the console, you can easily view any of the built-in reports that will show you the activity in your domain, including changes made to computers, Group Policy Objects (GPOs), groups, OUs, and users. If your company is audited regularly, you'll appreciate the prebuilt Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry

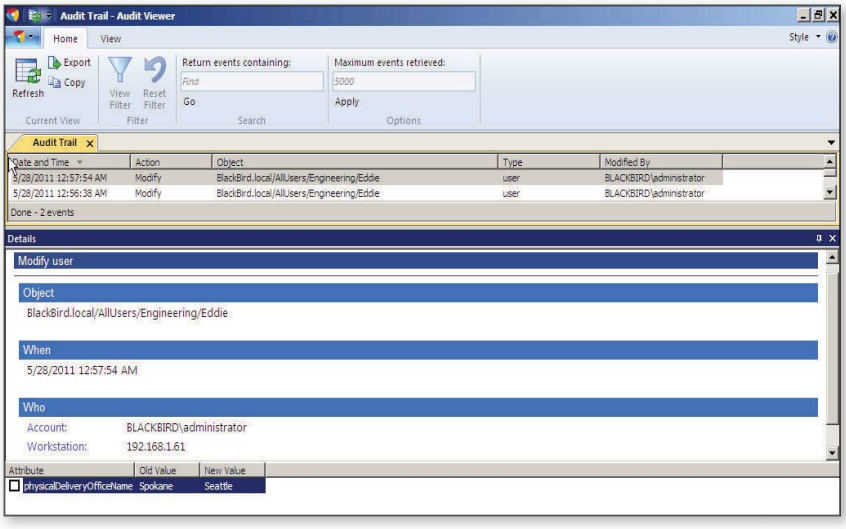


Figure 1: Displaying an audit trail in Blackbird Auditor for Active Directory

(PCI), and Sarbanes-Oxley (SOX) Act compliance reports.

If the built-in reports don't show what you're looking for, you can create your own. First, you create a new Audit View by answering a few *who, what, where,* and *when* type questions. Then, you schedule the audit. You can have the report emailed to you in .pdf or .xml format.

Reports are great for after-the-fact information, but there are certain events you need to know about right away. Blackbird Auditor can notify you when changes (create, modify, delete, move, and rename operations) are made to certain accounts or object types or when they occur on specific workstations or DCs.

Blackbird Auditor is tightly integrated with the MMC Active Directory Users and Computers snap-in. Installing the Blackbird RSAT Extensions adds several options to the snap-in. The *Show audit trail, Show account activity,* and *Show group membership changes* options are added to user objects. For example, right-clicking a user object and choosing *Show audit trail* displays what changes were made to objects and who made the changes, as Figure 1 shows. The *Show audit trail* option is also added to group and OU objects.

Blackbird Auditor is a simple yet powerful tool. When combined with one or more of the other Blackbird modules, it puts the tools needed to manage AD at administrators' fingertips.

Blackbird Auditor for Active Directory

PROS: Tight integration with the Active Directory Users and Computers snap-in; licensed on HR employee count, not AD user count

CONS: No built-in tool to assist in removing or archiving old data

RATING: ◆◆◆◆◇

PRICE: $6 per employee (HR count, not AD count)

RECOMMENDATION: Outstanding integration with the Active Directory Users and Computers snap-in and prebuilt FISMA, HIPAA, PCI, and SOX compliance reports make Blackbird Auditor stand out.

CONTACT: Blackbird Group • 866-224-8330 or 212-380-1465 •www.blackbird-group.com

ManageEngine's ADAudit Plus

Unlike the other products in this review, ADAudit Plus from ManageEngine (a division of Zoho) doesn't require a SQL Server or SQL Server Express database. Instead, a MySQL database is configured for you during installation. ADAudit Plus supports Win2K AD and later.

For this evaluation, I installed ADAudit Plus directly on the DC. However, in a production environment, you'll want to install it on a dedicated server. Licensing is handled through an XML file.

The installation took only a few minutes, and soon I was logging on to the admin console through a web page (port 8081

Table 1: Product comparisons

Company	Product	Price	Supported AD environments	Back-End Database	.NET Framework Version	Agent Based or Windows Event Logs	Database Purge and/or Archive	Built-In Regulatory Compliance Reports	Type of UI	Email notifications	Integration into the Active Directory Users and Computers Snap-In
Blackbird Group 866-224-8330, 212-380-1465 www.blackbird-group.com	Blackbird Auditor for Active Directory	$6 per employee (HR count, not AD count)	AD 2000 or later	SQL Server 2005 or later SQL Server Express 2008 (only for trial and production environments with up to 2 DCs and a maximum of 2,500 users)	.NET Framework 3.5 (with SP1) or later	Agent bypasses the event logs		FISMA, HIPAA, PCI, and SOX	MMC snap-in	Yes	Yes
ManageEngine (a division of Zoho) 888-720-9500, 925-924-9500 www.manageengine.com	ADAudit Plus	Ranges from $495 for 2 DCs to $19,995 for 200 DCs	AD 2000 or later	MySQL	Not required	Gathers data from the event logs (doesn't use agents)	Purges		Web console	Yes	
NetVision 877-828-9180 www.netvision.com	NVAssess	$15 per user (quantity discounts available)	AD 2003 or later (AD 2000 is supported under specific conditions, but it isn't recommended)	SQL Server 2008 or later SQL Server 2008 Express	Not applicable (comes preconfigured)	Agent bypasses the event logs	Purges and archives	HIPAA (PCI in development)	Application for setup Web console for reports	Yes	
NetWrix 888-638-9749, 201-490-8840 www.netwrix.com	Active Directory Change Reporter	$672 for 1 to 149 users, $5.95 per user for 150 or more users (quantity discounts available)	AD 2000 or later	SQL Server 2005 or later with SSRS required for advanced reporting SQL Server 2005 Express with Advanced Services	.NET Framework 2.0 or later	Agent gathers data from the event logs			MMC snap-in		
Quest Software 800-306-9329, 949-754-8000 www.quest.com	Change Auditor for Active Directory	$12 per enabled AD user (quantity discounts available)	AD 2000 or later	SQL Server 2005 or later	.NET Framework 4.0	Agent bypasses the event logs	Purges and archives	HIPAA, PCI, SOX, SAS 70, FISMA, and GLBA	Application	Yes	
ScriptLogic 800-813-6415, 561-886-2400 www.scriptlogic.com	Active Administrator	$15 per enabled AD user (quantity discounts available)	AD 2000 or later	SQL Server 2000 or later MSDE 2000 SQL Server 2008 Express SQL Server 2005 Express	.NET Framework 3.5 or later	Agent gathers data from the event logs	Purges		Application	Yes	

by default). The setup process was easy because the console walks you through each step. You just enter the name of your domain and DC, after which you edit the Default Domain Controllers Group Policy so that events are captured correctly. It's important to note that the events are gathered in batches instead of being captured in real time.

ADAudit Plus can be run as a standalone application (where you have to remember to start the program every time the computer is restarted) or as a service. Running the program as a service removes the requirement that you manually start the application every time the server is restarted.

Once logged on, a nice dashboard gives you an overview of recent domain activity, including logon failures, number of users locked out, peak logon hours, and the number of passwords that have been set or changed. You can drill down into each graph in the dashboard to see more detailed information. ADAudit Plus has one of the best dashboards of the products I reviewed.

The Reports tab is where you can really get into the meat of the data, as Figure 2 shows. The 33 built-in reports are grouped into 8 specific categories: User Logon Reports, Local Logon-Logoff, User Management, Group Management, Computer Management, Domain Policy Changes, OU Management, and GPO Management. There are no built-in regulatory compliance reports.

To create your own report, you click New Report Profile and fill out a simple query form. For example, I was able to easily create a report on all OUs that had been created, deleted, renamed, or moved; had their permissions changed; or had child objects added. Specific OUs can be targeted in the report, or the entire domain can be reported on.

If you want to be notified when something specific happens in the domain, you can configure web alerts or email alerts. For example, you can have ADAudit alert you when a logon failure occurs, a user or group is created or deleted, a domain policy is changed, or a GPO or OU is deleted.

I found that the user guide was a bit lacking. It wasn't terrible, but this web-based guide could have walked users through setup and administration better.

For basic Security event log reporting, ADAudit Plus is a great value. It does a good job of capturing the data and presenting it in a manageable format. I did find that it lacked the ability to capture before-and-after data, even though Microsoft now includes this capability in the Security event log in Windows Server 2008 and later. According to ManageEngine, this feature is in development and might be released by the time you read this.

ADAudit Plus

PROS: Price; dashboard gives a great overview of domain activity

CONS: User guide lacking; no built-in compliance reports; no before-and-after data; event log data not gathered in real time

RATING: ◆◆◆◇◇

PRICE: Ranges from $495 for two DCs to $19,995 for 200 DCs

RECOMMENDATION: For simple, cost-effective event log reporting, ADAudit Plus comes in at an extremely low price point.

CONTACT: ManageEngine, a division of Zoho • 888-720-9500 or 925-924-9500 • www.manageengine.com

NetVision's NVAssess

NetVision's NVAssess comes packaged differently than the other five products in this review. You can purchase NVAssess as a virtual appliance, a turnkey solution in the form of a 1U server appliance, or a managed service. NVAssess supports Windows Server 2003 AD and later. Although Windows 2000 Server AD is supported under specific conditions, it isn't recommended. NVAssess uses a SQL Server back end. SQL Server 2008 and SQL Server 2008 Express are supported.

The virtual appliance is supported in VMware ESX or ESXi 3.5 or later. There is also a version that can run in VMware Workstation 6.5. For this review, I downloaded the 8GB virtual appliance in the form of a file named SimonNV711-ESX.ova. I used a free VMware tool named OVF Tool (www.vmware.com/appliances/getting-started/learn/ovf.html) to properly import the SimonNV711-ESX.ova file into my VMware ESXi server.

The rest of the setup can be performed by you or NetVision technical support. NetVision recommends that you let its support staff assist you in the initial setup, as it can greatly reduce your ramp-up time and get the application working quickly. The cost for this service varies by the size

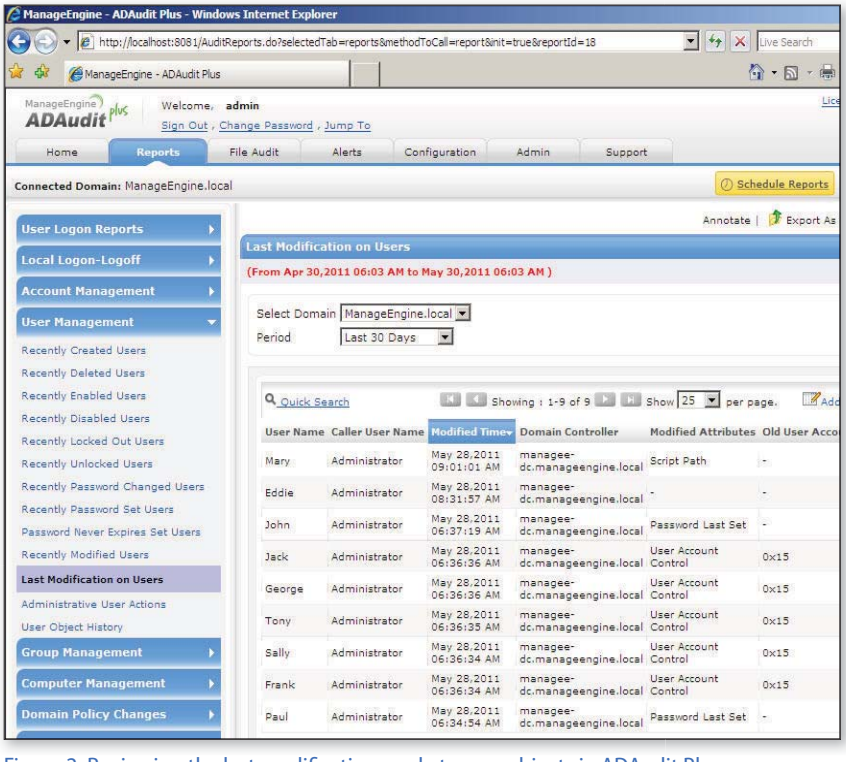


Figure 2: Reviewing the last modification made to user objects in ADAudit Plus

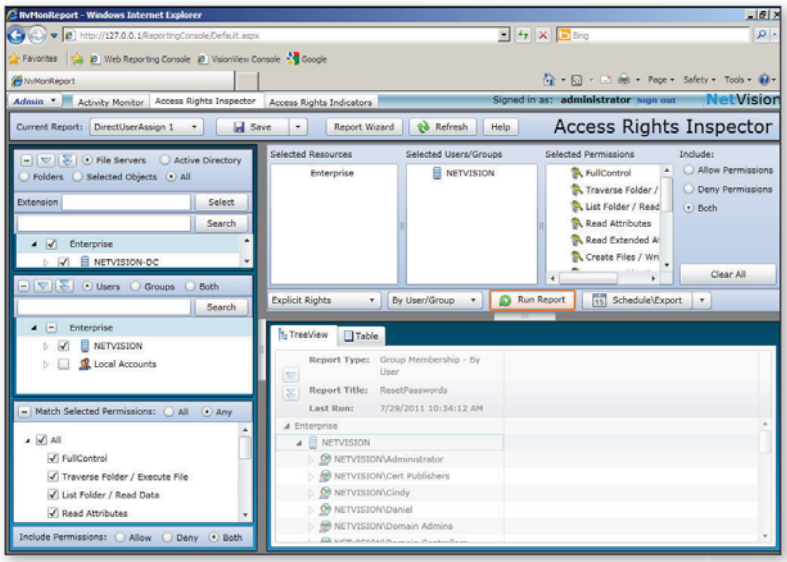


Figure 3: Working with raw data and reports in NVAssess's NvMonReport application

of your infrastructure, but you can expect to pay at least a few hundred dollars to more than a thousand dollars. Personally, I found the support folks to be extremely knowledgeable and personable, and they had me up and running in no time. In the overall scheme of things, a thousand dollars isn't that big of a deal and it's money well spent.

When I called tech support, the technician had me use a screen-sharing program called Team Viewer so that he could connect to my NVAssess appliance. I watched as the technician manually installed the required agents onto each DC. NetVision wrote these agents to interact with AD directly (bypassing the event logs) and use Microsoft's Background Intelligent Transfer Service (BITS) to transfer the activity data back to the SQL Server database. While the agents were installing, we had a nice discussion about using Group Policy and transform files (using the free transform creator, Orca) to automate the agent-installation process. I have a feeling that you might see this method in the next version of the appliance.

As the technician continued to configure the software, he explained that the purpose of the setup service is to not only make sure everything is working correctly but also assist the customer in getting the most out of the software. For example, although there are some built-in HIPAA templates, the technician was very interested in what I wanted to monitor and was more than willing to help me get the data that I (or perhaps more important, the auditors) need.

The virtual appliance runs Server 2008 Standard Edition on 32-bit virtual hardware (two CPUs and 4GB of memory). Although the server itself is 32-bit, the DC agents come in both 32-bit and 64-bit versions. SQL Server 2008 Express is installed, but you can upgrade it to a full version of SQL Server 2008 or point the appliance to an existing instance.

Because NVAssess comes preconfigured in the appliance, the setup is already done for you. Your only immediate tasks are to change the IP address to match your environment and to add the server's A record to your internal DNS infrastructure. Changing the name of the server and adding it to the domain is supported but not recommended because it can break some of the preconfigured settings in the appliance. These settings can be fixed, but it causes extra work for you.

In addition to monitoring AD, NVAssess can monitor Microsoft Exchange Server, file servers, Network Appliance (NetApp) SANs, and even Novell eDirectory. You use two utilities for monitoring: the NetVision Administration Console, a 32-bit program that runs on the virtual or server appliance, and NvMonReport, a web-based application that can be accessed from any browser.

The NetVision Administration Console is where you choose what you want to monitor in AD. You simply drag a policy template from the Template area to the Policy area, where you define it. Policies can include and exclude attributes of AD objects that you want to monitor. For example, you can create a policy that monitors all user changes (which includes user logons) or a policy that monitors all user changes, except user logons. After you define and enable the policy, NVAssess immediately starts monitoring AD for the specified conditions.

Raw data and reports can be viewed in NvMonReport, which Figure 3 shows. A Report Wizard walks you through creating reports on effective rights (who has access to what), explicit rights (who has actual rights, not inherited rights), group membership, delegated control, direct user assignments (where a user, not a security group, has been granted access), and denied entries (where permissions have been explicitly denied).

If the reports aren't exactly to your liking, the NetVision support staff can help you tweak them. I found the reports to be very granular. If you need to receive the reports via a schedule, NVAssess can send them to you in .pdf or .xls format. If you want NVAssess to act immediately when it detects nefarious activity, you can set up an Action item that runs either a Visual Basic (VB) or C# script.

Overall, I was impressed with the product. It's extremely robust and not simply a canned, one-size-fits-all application. Although the initial cost and setup time might be a turnoff to some people, those who desire a custom solution will appreciate not being boxed in. If you desire a partner that will work with you on your AD auditing solution, NetVision would be a good choice.

NVAssess

PROS: Offered as a turnkey solution (1U server appliance), a managed service, or as a virtual appliance; robust reporting capability; technical support walks you through system configuration

CONS: Potentially high startup costs; event log data not gathered in real time

RATING: ◆◆◆◆◆

PRICE: $15 per user (quantity discounts available)

RECOMMENDATION: NetVision should be your first choice if you're looking for a turnkey solution. No matter whether you want to use the physical appliance, virtual appliance, or managed service, it's the best for hands-free AD auditing.

CONTACT: NetVision • 877-828-9180 • www.netvision.com

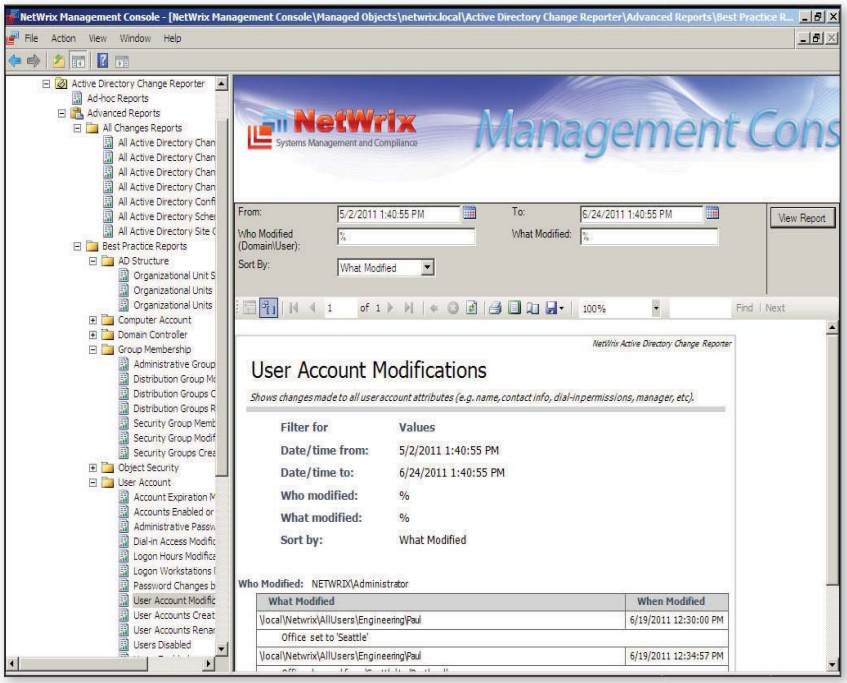


Figure 4: Browsing through the built-in reports in Active Directory Change Reporter

NetWrix's Active Directory Change Reporter

Active Directory Change Reporter is a sister application to other Change Reporter tools offered by NetWrix. I reviewed Group Policy Change Reporter last year ("NetWrix Group Policy Change Reporter," June 2010, InstantDoc ID 125023) and immediately felt at home with the interface of Active Directory Change Reporter. It's easy to navigate and understand.

Active Directory Change Reporter supports Win2K AD and later. It can be installed on a DC or XP or later workstation as long it's a member of the domain. I chose to install it on the same server on which I installed SQL Server. Active Directory Change Reporter supports SQL Server 2005 or later. SQL Server 2005 Express is also supported, but you must have the version that includes Advanced Services.

Setting up the product is quick and easy. However, getting all the prerequisites out of the way can take some time and configuration. Because I was using Server 2008 in the test lab, the automatic configuration wizard in the setup routine didn't work. This is a known problem, so I had to follow special instructions that guided me through manually setting up SQL Server 2005 Express with Advances Services and IIS 7.0. The same wizard helps you configure the license, deploy agents to DCs, adjust the audit policy settings on the DCs, enable long-term archiving, and more. It also helps you change the tombstoneLifetime property from 180 to 744 days so that deleted AD objects can be restored.

As soon as the setup was complete, I was able to quickly generate the report. As Figure 4 shows, the left side of the management console guides you through finding the report that you need. There are 38 prebuilt reports, including reports on schema changes, site changes, and AD changes by date, object type, or user.

A unique feature of Active Directory Change Reporter is the Best Practice Reports. These reports are broken into six subcategories: AD Structure, Computer Account, Domain Controller, Group Membership, Object Security, and User Account. For example, under AD Structure, a prebuilt report titled Organizational Units Created can help you determine whether a rogue administrator is creating unnecessary clutter in your domain. Another report under Group Membership shows who has been added or removed from security groups or Distribution Groups (DGs). Each report helps you keep a handle on the changes being made to the domain.

If these reports don't show you the data that you require, Active Directory Change Reporter uses Microsoft's SQL Server Reporting Services (SSRS) to store the data gathered from DCs. This is why you must ensure that SQL Server 2005 Express is installed with Advanced Services. With SSRS, you can quickly adjust the built-in reports and get the data you need.

A feature above and beyond basic reporting is the Restore Wizard. Using either standard AD tombstone data (AD objects that have been marked for deletion but haven't been purged from the database yet) or NetWrix snapshots, you can easily restore individual objects without restoring the entire AD database.

As I mentioned previously, Active Directory Change Reporter is a sister application to other NetWrix products. Combined with these other easy-to-use tools, you have a real powerhouse.

Active Directory Change Reporter

PROS: Easy-to-use and -understand interface; very similar to the other NetWrix Change Reporter tools; SSRS back end makes the data easily accessible

CONS: Event log data not gathered in real time; no built-in compliance reports; no built-in database purge or archive capability; no email notification capability

RATING: ◆◆◆◇◇

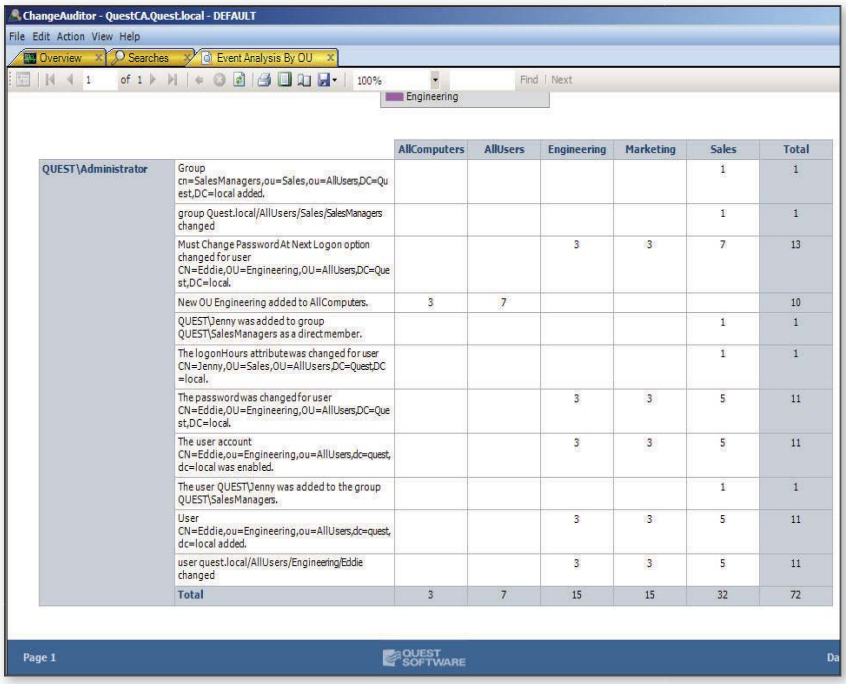
PRICE: $672 for 1 to 149 users, $5.95 per user for 150 or more users (quantity discounts available)

RECOMMENDATION: If you need a full suite of change reporting tools, NetWrix is a great choice.

CONTACT: NetWrix • 888-638-9749 or 201-490-8840 • www.netwrix.com

Quest Software's ChangeAuditor for Active Directory

Quest Software's ChangeAuditor for Active Directory is great at helping you view, manipulate, and really dig into the data that it gathers about the activity on your domain. It supports Win2K AD and later, and consists of four components:



		AllComputers	AllUsers	Engineering	Marketing	Sales	Total
QUEST\Administrator	Group cn=SalesManagers,ou=Sales,ou=AllUsers,DC=Quest,DC=local added.					1	1
	group Quest.local/AllUsers/Sales/SalesManagers changed					1	1
	Must Change Password At Next Logon option changed for user CN=Eddie,OU=Engineering,OU=AllUsers,DC=Quest,DC=local.			3	3	7	13
	New OU Engineering added to AllComputers.	3	7				10
	QUEST\Jenny was added to group QUEST\SalesManagers as a direct member.					1	1
	The logonHours attribute was changed for user CN=Jenny,OU=Sales,OU=AllUsers,DC=Quest,DC=local.					1	1
	The password was changed for user CN=Eddie,OU=Engineering,OU=AllUsers,DC=Quest,DC=local.			3	3	5	11
	The user account CN=Eddie,ou=Engineering,ou=AllUsers,dc=quest,dc=local was enabled.			3	3	5	11
	The user QUEST\Jenny was added to the group QUEST\SalesManagers.					1	1
	User CN=Eddie,ou=Engineering,ou=AllUsers,dc=quest,dc=local added.			3	3	5	11
	user quest.local/AllUsers/Engineering/Eddie changed			3	3	5	11
	Total	3	7	15	15	32	72

Figure 5: Analyzing events by OUs in ChangeAuditor for Active Directory

- The ChangeAuditor Coordinator
- The ChangeAuditor Client
- ChangeAuditor Agents
- A SQL Server database

The first step is to install the Coordinator. The Coordinator gathers all the events that the Agents send and can be installed on the same machine as SQL Server or on a separate server. The installation is quick and painless.

After the Coordinator is installed, you need to install the Client on the same server as the Coordinator or on a separate management computer. The Client application is where you will spend all of your time.

Next, you need to install an Agent on each DC so that it can monitor that domain's activity. Installing an Agent is easy. Using the ChangeAuditor application, you simply right-click the server (or servers—using the Shift key allows multiple servers to be selected), click *Install or Upgrade,* and enter credentials with administrative privileges. The install takes just a few minutes to complete. No further configuration of the Agents is necessary.

The Client console is simple to navigate and makes it easy to break down and dig into the raw data. Gathering details about events is clean. Before and after values show you exactly what was changed.

If you need to provide information to non-IT personnel, you'll appreciate the reports that are ready to go out of the box. All you need to do is run the reports to provide the non-IT personnel with answers to questions such as "Who has been adding OUs?" and "Who has been altering user accounts?" as Figure 5 shows. For those of you who have to worry about compliance to HIPAA, PCI, SOX, Statement on Auditing Standards (SAS) 70, and Gramm-Leach-Bliley Act (GLBA), the product's prebuilt reports can help you convince auditors that you really do have your ducks in a row. Creating your own reports, however, isn't as intuitive as some of the other products and takes a little getting used to.

Now that you have easy access to this data, what does it all mean? Quest provides a robust knowledge base that's directly linked to security events. When you right-click an event and choose *Knowledge base,* a web page appears, explaining what the event means in detail.

As you gather data over the months, you might want to eventually move old records from the database to an archive. Under the Administration Tasks tab, you can easily set up a task that can archive, purge, or archive then purge records. When purging records, you can select records older than a specific date and records that meet specific criteria, such as events that contain a specific string or events from specific computers, domains, users, or groups. Database archives can be saved by calendar month, quarter, or year.

If you need to really dig into the AD data, ChangeAuditor puts the necessary tools at your fingertips. For an additional charge per Agent, you can even have Change Auditor monitor Exchange, file servers, SQL Server, NetApp SANs, and EMC SANs. It requires SQL Server 2005 or later and .NET Framework 4.0.

ChangeAuditor for Active Directory

PROS: Great tools to help you really dig into the data; events link to an online knowledge base that clearly explains what they mean

CONS: Creating custom reports isn't as intuitive as it could be

RATING: ◆◆◆◆◇

PRICE: $12 per enabled AD user (quantity discounts available)

RECOMMENDATION: If you need more than just pretty reports, ChangeAuditor for Active Directory should top your list.

CONTACT: Quest Software • 800-306-9329 or 949-754-8000 • www.quest.com

ScriptLogic's Active Administrator

Like the other five products, ScriptLogic's Active Administrator requires a database to store security events. Unlike the other five products, Active Administrator is by far the most flexible in this area. It supports SQL Server 2000 and later, Microsoft Data Engine (MSDE) 2000, and the newer SQL Server Express database engines. Also unlike the other products, Active Administrator utilizes the Group Policy Management Console (GPMC), so this must be installed as well as .NET Framework 3.5. It supports Win2K AD and later.

The first step is to install the Active Administrator Server software. This needs

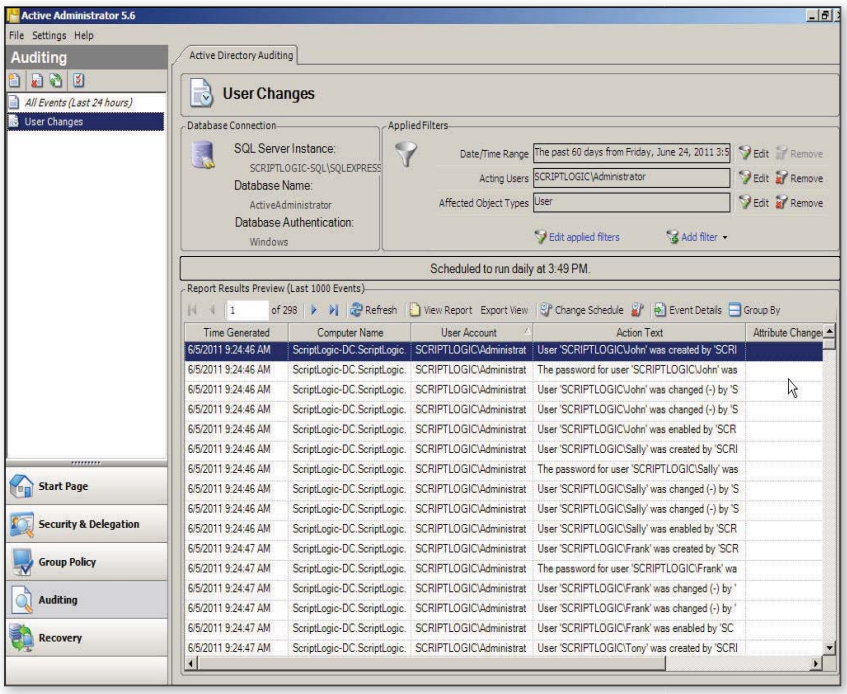


Figure 6: Filtering events in Active Administrator

to be installed on only one server. The installation routine quickly walks you through configuring the license file, creating the database, and configuring SMTP, service account passwords, and AD backup and restore settings.

Next, auditing needs to be enabled on each DC. The easiest way to do this is with the Default Domain Controllers Policy. The Active Administrator Installation Guide walks you through the specific audit policy settings that need to be adjusted. Once the policy has been edited, you need to run the *gpupdate /force* command on each DC.

To collect information from the event logs, you use the Active Administrator application to deploy the Collection Agent to each DC. Finally, you install the Active Administrator Console on any machine (e.g., your administration workstation).

The first thing you notice about Active Administrator is that this application does much more than just AD auditing. It includes many tools that AD administrators need to use daily. All the features and tools that Microsoft forgot to put into the Active Directory User and Computers snap-in and GPMC are included in Active Administrator. For example, after using the Delegate Control feature in the Active Directory User and Computers snap-in, you quickly realize that it's really a one-way tool. You can easily delegate permissions, but revoking them or even understanding what permissions you have granted is challenging. Active Administrator cleans up what Microsoft left behind. Revoking permissions is as easy as delegating them. If auditors ask you to demonstrate who has special permissions in AD, a report is just a click away.

Active Administrator has some impressive Group Policy management features as well. Group Policy gives you great power that can make your job easier, but that power can also cause "Resume Generating Events (RGEs)." Active Administrator's Group Policy Rollback feature helps you quickly undo the mistake and get the network back to normal.

Another bonus feature is the password-restore tool. If your domain is running Windows 2003 SP1 or later, Active Administrator can restore the password of deleted users or computers. This does require a minor change to the Unicode-PWD object's searchFlags attribute in AD. (Note that this isn't a schema change but rather a simple attribute change.)

To view the data that's gathered from the DCs, you can click the Create New Report option to retrieve the last 1,000 events. You can then apply filters, such as Date/Time Range, Acting Users, and Affected Object Types. Figure 6 shows how easy it is to add filters. When you have the data you need, you click View Report to view the data. The report can be easily scheduled from this screen as well.

One notably missing feature is built-in regulatory compliance reports. However, ScriptLogic offers such reports in a separate product named Enterprise Security Reporter. Like most of the other products, Active Administrator can alert you via email when a specific event occurs.

Active Administrator

PROS: Simple interface; includes additional security, delegation, and Group Policy tools

CONS: High price; no built-in regulatory compliance reports

RATING: ◆◆◆◆◇

PRICE: $15 per enabled AD user (quantity discounts available)

RECOMMENDATION: If you need an audit tool and you like the bonus utilities that are included, give Active Administrator a try.

CONTACT: ScriptLogic • 800-813-6415 or 561-886-2400 • www.scriptlogic.com

Editor's Choice

Each of the six AD auditing tools gives you features well above and beyond what Microsoft includes in Windows Server and AD. Whether you need to track down that rogue user who is constantly testing the limits of your security or prove to an auditor that your systems are in compliance, you can't go wrong with any one of them. Each one has its own strengths and weaknesses, but the one that impressed me the most was NVAssess, which is why it earns the Editor's Choice award. ◆

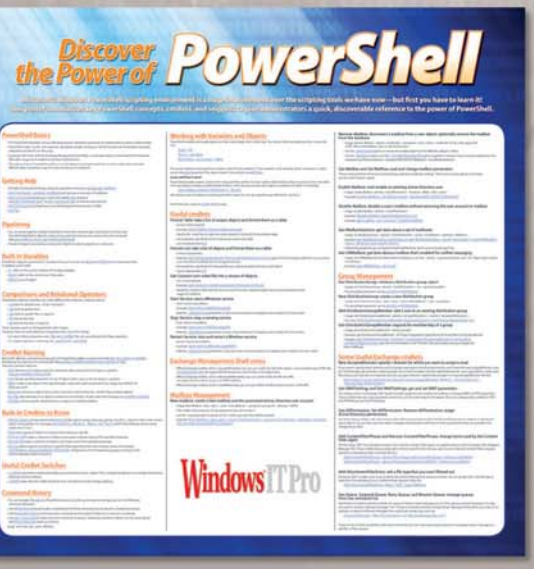
InstantDoc ID 139873

Eric B. Rux
(ebrux@whshelp.com), Windows Home Server MVP, is a contributing editor for *Windows IT Pro* and writes a monthly column at svconline.com/connectedhome/windowshomeserver. Eric is the manager of technical support services at Eastern Washington University.

Prime Your Mind

with Resources from Left-Brain.com

Left-Brain.com is the online superstore stocked with educational, training, and career-development materials focused on meeting the needs of IT professionals like you.



Featured Product:

Windows PowerShell Poster
Discover the Power of PowerShell

Microsoft's Windows PowerShell scripting environment is a huge improvement over other scripting tools, and we can help you learn it! Our new PowerShell poster summarizes key PowerShell concepts, cmdlets, and snippets for group management, Exchange, and other admin tasks.

Topics covered are PowerShell basics, pipelining, built-in variables, mailbox management, command history, and much more!

Only $14.95*!

Order your poster and discover other great PowerShell resources now at Left-Brain.com

left-brain

*Plus shipping and applicable tax.

www.left-brain.com

Windows IT Pro

How to Launch Your Company on the Cheap

Rent and virtualize your way to almost zero overhead

by Paul Thurrott

In the mid-1990s, I joined a San Francisco Bay area technology startup. In those days—before smartphones, let alone widespread laptop usage—most budding businesses proceeded down a pretty predictable path. They'd rent office space; buy Aeron chairs and other office equipment; install a phone system; hire office staff, marketing, and technical people; and install a network of PCs. Employees were paid actual salaries and were often promised a percentage of the company in the form of stock options and other incentives.

Given the ubiquity of wireless, broadband Internet access, smartphones, tablets and truly portable computers, and cloud computing services, that startup mentality seems almost quaint today—and it's possible to start a company now with virtually none of that overhead. You're no more likely to be successful now than you were in that earlier era, but you can funnel whatever little capital you do have toward your actual business—the processes and products you should be focusing on—instead of infrastructure.

Whether you're a fledgling startup with the next killer idea, a small business serving local customers, a growing entity with a multi-locale or international footprint, or even one of the world's largest enterprises, your critical business resources are being stretched in multiple directions. But with the advent of so many new technologies, the time has come to focus on what's truly important to your business. It's time to focus *on* your business and offload as much of the unnecessary bric-a-brac to other services, web or otherwise. We've been talking about such things for years. But unlike the dream of a paperless office decades ago, this time it's not just talk: It's possible today to safely, securely, and seamlessly offload a lot of your non-core business processes—and even some core, mission-critical needs. Many Market Watch columns focus on buying recommendations, but I'm taking the opposite tack and discussing what *not* to buy.

On-Premises Servers

The good old days: flying to San Jose so I could reach a stick into a server cage and reboot a single errant web server. Jealous? You can implement a modern version of this silliness by buying, deploying, and managing your own servers and server software. But why? Servers are expensive, loud, and complex, and they require a certain level of expertise, either from your own employees or via a support contract.

Modern new businesses should seek to minimize or eliminate their exposure to in-house server hardware. With the possible exception of centralized, local storage and, for large organizations, user management, there's little need for this complexity and cost. Small businesses should look at the recently released Microsoft Windows Small Business Server (SBS) 2011 Essentials (www.microsoft.com/oem/en/products/servers/Pages/windows_sbs_2011_essentials_overview.aspx), which can integrate with various online services while providing just the basics in-house. And with various cloud storage services, as well as PC management services such as Windows Intune (www.microsoft.com/windows/windowsintune), even the remaining excuses for on-premises servers are starting to fade.

PCs

If you thought the elimination of local server hardware was shocking, you're going to want to sit down. For a growing generation of startups, even corporate-funded PCs are going by the wayside, replaced by employees' own PCs. This isn't as radical as it sounds, and if you sign up for a PC management service such as Intune—starting at $11 per PC per month—you can easily manage these employee-owned PCs too, ensuring that they're up-to-date with software updates and security fixes. And in Intune 2.0, coming this year, you'll even be able to remotely deploy software to those PCs.

Another issue is whether everyone even needs a PC. Depending on the business and employees, a smartphone might be enough, especially for sales people or other frequent travelers. Even an iPad (www.apple.com/ipad) or other tablet device might work.

Email, Contacts, Calendar, and Tasks

If you're not an email service provider but you still host your own email servers, you're either constrained by regulatory or legal reasons, or you're just wasting time and money—especially now that there are inexpensive (even free) and high-quality choices for email and personal information management (PIM).

For young, new, and very small businesses, Google Apps (apps.google.com) is a good choice for email, contacts, calendar, and task management—and it's free for businesses with five or fewer employees. Google Apps provides email with a customized domain, and its services are broadly compatible across devices. The primary interface is via the web, but users can also use popular email clients such as Microsoft Outlook, although support for other Google Apps services in native apps is mixed.

Microsoft has a very viable alternative for cloud-based email, contacts, calendar, and task management: Office 365 (office365.com). Although there's no free option, it's cheap—starting at $6 per user per month—and it's much more powerful and full-featured than the Google offering. Office 365 also includes integrated Microsoft Office SharePoint Server (for document collaboration and sharing) and Microsoft Lync (for presence and online communication). It's Google Apps for grownups.

If you're really cash-strapped and not a fan of Google, Microsoft does have you covered, although you'll give up the power of Microsoft Exchange Server, SharePoint, and Lync: The company offers businesses a custom domain through its Windows Live Admin Center (admin.live.com), providing Hotmail-based email, contacts, calendar, and task management through the web, native Windows apps, and many mobile clients. (Hotmail is Exchange ActiveSync–compliant for device use.) You'll have to pay for your domain, but everything else is free.

Office Productivity Software

Speaking of Office, it's worth pointing out that although Microsoft Office 2010 (office.microsoft.com/en-us/suites) is a mature, highly capable Office productivity suite, it might be overkill for some people. Fortunately, there are free alternatives, and there's no reason you can't mix and match free and paid offerings, depending on your needs.

The best and most obvious of the free Office alternatives is actually another version of Microsoft Office called Office Web Apps (office.microsoft.com/en-us/web-apps). As its name suggests, this service offers web-based versions of Microsoft Word, Excel, OneNote, and PowerPoint, and although they're not as powerful as the native apps, and they can't work while you're offline, they look and work just like the real thing and could offer enough horsepower for many users. The Office Web Apps are free and come with Windows Live SkyDrive (skydrive.live.com—Microsoft's cloud storage solution, with 25GB of free storage), Office 365, and SharePoint 2010.

Google converts should check out Google Docs (docs.google.com), which provides web-based word processing, spreadsheet, and presentation solutions. That said, I find these web apps fairly lackluster compared with Microsoft's offerings, and you'll experience fidelity issues if you try to share documents between Office and Google Docs, which isn't an issue for Office Web Apps users.

Office Space

Let's not stop with Office software: For new and very small businesses, an actual office often isn't required at all. But thanks to new services, even the smallest business can appear to be big and successful. The key here is to do what bigger companies already do for satellite locations, and rent space where you can drop in at set times for meetings with potential and current clients and perform other face-to-face duties.

Many of these occasional office space services provide a permanent address for your business (where mail and packages can be routed and collected), a permanent receptionist crew, a phone that rings, and calls that are directed to the correct employees, no matter where they are and what kind of phones they use. An entry-level package that grants companies 5 days of office space per month, along with the mailing address, receptionist, and phone services, should cost about $200 a month—a far cry from the rental fees on a permanent address.

These services are available in various locations. One that I'm familiar with in Seattle is called ThinkSpace (thinkspace.com). It offers lobby company name boards—many with the same suite numbers, of course—and environmentally friendly "green" messaging. The rest of the time, employees can perform their duties remotely, as usual, and use services such as GoToMeeting or Microsoft Lync (part of Office 365) for virtual meetings.

Customer Support

While we're talking about virtualizing your physical infrastructure, you should also consider virtualizing your customer support, eliminating yet another round of costs and overhead. Zendesk (support.zendesk.com) presents an inexpensive option: The company logs customer support cases, ties into your email system, generates support tickets, and so on. It's a grab-and-go solution.

Phones

Another way to make your business appear larger and more professional is to implement a virtual phone system, such as that offered by Grasshopper (grasshopper.com). This completely web-based service provides 800 numbers for customer support and sales, local numbers for geo-diversity, hold music, and call routing to any phone—starting at just $10 per month. Google goers should look into Google Voice, although it's geared toward both individuals and small businesses.

Send Me Your Tips!

There are many excellent ways for up-and-coming companies to save money, and I'm sure I've only scratched the surface here. If you have some tips of your own, please email me (paul@windowsitpro.com), and I'll look at compiling them for a follow-up article.

InstantDoc ID 139892

Paul Thurrott
(paul@windowsitpro.com) is senior technical analyst for *Windows IT Pro*. He writes the SuperSite for Windows (winsupersite.com), a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email), and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

VMware Replication Solutions

Ensure virtual business connectivity in the event of a disaster

by Zac Wiggy

Virtualization has a lot of benefits. You save power, make better use of existing hardware—you know the spiel. But it also comes with some increased risks, because you're putting your eggs into fewer baskets. If you have a hardware failure or virus infection in a host, you also have problems for all the virtual machines (VMs) running on the host. That means that in a virtual environment, you not only need to make sure that all your VMs are getting backed up properly, you also have to be certain that losing one host doesn't mean your entire IT environment will be out of commission.

There are many choices for products to help you replicate your VMware environment, so start with the buyer's guide table accompanying this article to get an idea of what's out there. Take a thorough inventory of what you have and what you need before you start shopping so you know you're headed in the right direction.

Basic backup hardware considerations, including storage capacity and performance, are as important in a virtual environment as anywhere. However you're replicating and wherever you're replicating to, make sure your drives can handle the data. If you're going for more than simple backups, you also have to make sure that your network and server hardware is up to the task. If you want a replication system with automatic failover, make sure you actually have the capacity to fail over your VMs. If you don't have the computing power, you could have one host crash, then when its VMs fail over to the next, that host could become bogged down and unusable.

Licensing can be one of the trickier aspects of virtualization, and licensing a VMware replication product is no exception. In the sampling of products in the accompanying table, there are products licensed on a per-server or per-host, per-VM, per-CPU-socket, and per-terabyte-of-storage basis. Before committing to a product, be sure you know the terms under which you're getting the product and what you'll need to pay if your needs change.

Inventory your hosts and VMs carefully so that the product you choose covers all of the OSs you use. Another consideration is whether the product will help you back up a mixed hypervisor environment—Microsoft's Hyper-V is seeing use in many IT test environments and is also moving into more and more production environments. If you're planning on using more than one hypervisor, or if you'd just like to leave the option open, don't forget to include that factor in your decision.

Cloud replication is a feature you should consider carefully. Offsite storage can save your data in case of an emergency, and knowing that your data is regularly being stored with your service provider can provide a lot of peace of mind. On the other hand, cloud storage isn't the best option for every environment. Local storage is very inexpensive these days, and cloud storage space can sometimes be substantially more expensive. You might also be located somewhere with limited bandwidth. And cloud storage can raise serious legal questions, especially when data would be stored in a country other than the one where you're located. If the country where you're storing your data has laws allowing its government to seize the data—as the United States does—you could face problems with your own government. Many industries also regulate where you can store your data, so you might have to get your company's legal department involved with this decision.

Even a casual glance at this month's buyer's guide table will show you that you have a lot of choices in this area, and the products have big differences between them. There are also many different licensing models and price levels. A good replication setup can keep your computers running after a disaster, but a bad one will only lull you into a false sense of security, making a disaster that much worse.

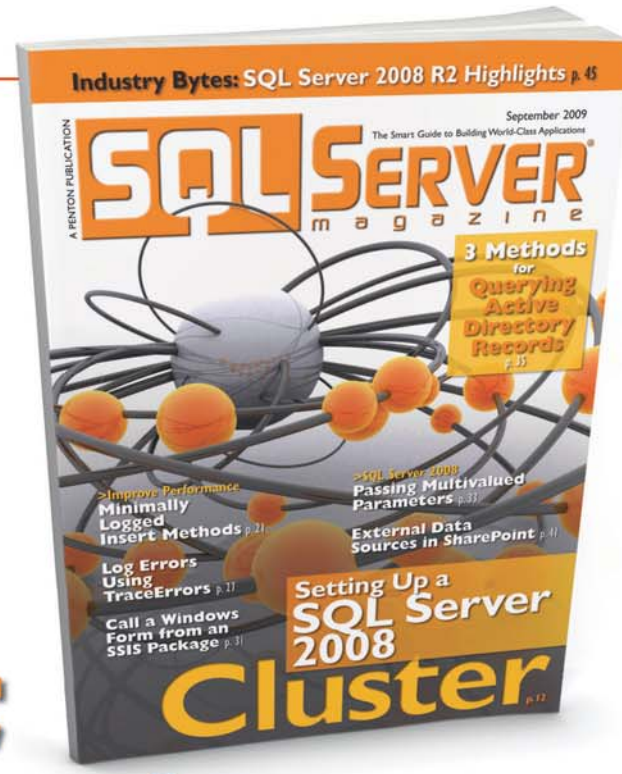
InstantDoc ID 139868

Zac Wiggy
(products@windowsitpro.com) is the former products editor for *Windows IT Pro* and *SQL Server Magazine*. Zac has more than 7 years experience as a technology journalist, newspaper reporter, and editor.

Company	Product	Licensing	VMware Environments and Versions Supported	Other Virtualization Environments Supported	VM OSs Supported
CA Technologies 800-225-5224 www.ARCserve.com	CA ARCserve Replication and High Availability	Per-server, per-host, per-socket and per-TB capacity options	VMware ESX, Vsphere 3.x	XenServer and Hyper-V	Windows Server 2008, 2003, Linux and Solaris x86/x64
CommVault 888-746-3849 www.commvault.com	Simpana 9	Two options; specifics dependent on licensing options	VMware ESX/ESXi 3.5 and later	Hyper-V and XenServer	All guest OSs supported by hypervisor
FalconStor Software 631-777-5188 866-669-3252 www.falconstor.com	Continuous Data Protector (CDP) with RecoverTrac	$2,000 to $6,000 per TB	VMware ESX, ESXi, vSphere	Hyper-V	Contact vendor
Hitachi Data Systems 408-970-7568 www.hds.com	Hitachi TrueCopy Remote Replication (Modular) Hitachi Universal Replicator (Enterprise)	Licensed per TB	VMware vCenter Site Recovery Manager 4.0, 4.1	Storage devices when virtualized behind Hitachi's Universal Storage Platform (USPV/VM) + Virtualized Storage Platform (VSP)	Please check VMware's Support Matrix
InMage Systems 408-200-3840 800-646-3617 www.inmage.com	Scout	Starting at about $4,500; licensed at vSphere host level and tiered based on guest VM count	VMware ESX and ESXi, versions 3.5, 4.0, 4.1 and all update levels	XenServer and Hyper-V	Windows Server 2008, 2008 SP2, 2008 R2, 2008 R2 SP1, 2003, 2003 R2, Redhat Enterprise Linux
Quest Software 949-754-9177 www.quest.com/vranger	vRanger Backup and Replication	$699 per CPU socket	All shipping and supported VMware vSphere versions vSphere 3.5, vSphere 4, 4.1, 4.1 Update 1	None	All VMware supported guest OS
Symantec 650-224-6974 800-721-3934 www.symantec.com	Symantec Backup Exec 2010 R3	$1,224 for Backup Exec Media Server, $1,962 for Backup Exec Agent for VMware; Backup Exec Media Server is licensed per backup server, Agent for VMware is licensed per ESX or vSpere host.	VMware ESX 3.5 Update 2 and above; vSphere 4.x	Hyper-V 2008, Hyper-V 2008 R2, Citrix virtualization when protecting virtual guests with an Agent within each guest	Windows 2000 and later (both 32-bit and 64-bit), Red Hat 5.x, SLES 11.x, SLES 10.x
	Symantec ApplicationHA	$350/VM; doesn't provide replication—integrates with VMware Site Recovery Manager to provide application awareness in SRM environments	VMware vSphere 4.0 and 4.1 and SRM 4.1.	None	Windows Server 2008, 2008 R2, 2003, 2003 R2 (all x64); Server 2003, 2003 R2 (32 bit); Linux x64 (RHEL 5, SLES 11 SP1, OEL 5)
Veeam Software 614-339-8200 www.veeam.com	Veeam Backup & Replication	$599 per socket for Standard; $899 for Enterprise Edition	vSphere 4.x, VMware Infrastructure 3.x (VI3), ESX 4.x and 3.x, ESXi 4.x and 3.x, vCenter Server 4.x (optional), Virtual Center 2.x (optional)	Hyper-V support in Q4	All OSs supported by VMware

	Real-Time, Scheduled, or Batched Backups	Automatic Failover or Fallback	Transport Mechanism	Support for Multiple Replication Targets	Automatically Update DNS Entries	Cloud Backup Support	CDP Support	VM Image Restore or File-Level Restore
	Real-time, scheduled, batched	Both	Host level, asynchronous, byte level replication over LAN/ WAN with support for offline seeding of data	Yes	Yes	Amazon EC2 and many private clouds	Yes	File-level restore
	Real-time, scheduled, batched	Automatic failover	HW-based replication, TCP/IP, SAN, hot add, NAS, NDB, NBD SSL	Yes	Yes	Amazon S3, AT&T Synaptic Storage, Microsft Azure, Rackspace, EMC Atmos, Nirvanix	Yes	Both
	Real-time, scheduled, batched	Both	Fibre Channel, iSCSI, FCoE	Yes	Yes	FalconStor MSPs	Yes	Both
	N/A	Automatic failover	Fibre Channel (Block Based Replication) + TCPIP (SRM Communication)	No	No	No	No	VM image
	Real-time	Both	Proprietary replication protocols over TCP/IP.	Yes	Yes	Hardware agnostic (any cloud platform)	Yes	Both
	Real-time, scheduled, batched	Automatic failover	FIbre Channel LAN (NFS/ CIFS/iSCSI), WAN	Yes	No	Through hybrid backup-to-cloud appliances	No	Both
	Scheduled, batched	No	SAN, NBD, NBDSSL, HOTADD	Yes	No	Can protect data to the Nirvanix Cloud	No	Both
	N/A	Automatic failover	VMware Site Recovery Manager's transport mechanism	No	No	No	No	N/A
	Real-time, scheduled, batched	No	TCP/IP	Yes	No	Yes, several cloud partners	No	Both

Editor's Note: Some vendors you might expect to see in this Buyer's Guide said they didn't have a product that exactly matched the criteria or didn't respond to our requests for information about their products.

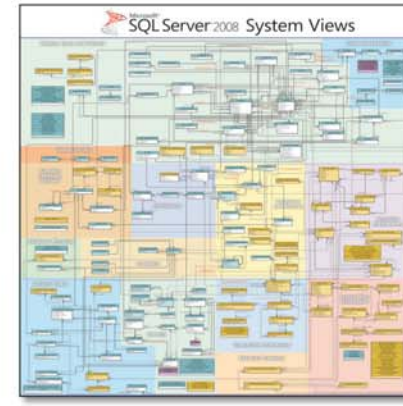


Get SQL Server Magazine @ 58% Off the Cover Price!

Only $29.95*—it's like getting every other month FREE!

5 More Reasons You Won't Want to Miss a Single Issue:

- **ACCESS TO EXPERTS:** Solve your toughest IT headaches with in-depth columns by Kalen Delany, Itzik Ben-Gan, and Brian Moran.
- **UP-TO-THE-MINUTE:** Comprehensive coverage of T-SQL, Reporting Services, log files, business intelligence, SharePoint, and much more.
- **COMMUNITY-WIDE RESOURCES:** Access to blogs, forums, Web updates, events and news alerts on the absolute latest industry developments as they happen.
- **EXCLUSIVE ACCESS:** Subscriber-only access to the entire *SQL Server Magazine* online article database.
- **RISK-FREE OFFER:** If you're not satisfied with *SQL Server Magazine* at any time, simply cancel your subscription and receive a refund for any un-mailed issues.



We'll also send you the latest SQL Server 2008 System Table Map Poster FREE with your paid order!

Start Your Subscription Now at SQLMag.com/go/sqldev

SQL SERVER magazine

*Rates vary outside the U.S.

INSIGHTS FROM THE INDUSTRY

Is Mobile Application Management the New Mobile Device Management?

Mobile device management (MDM) is the concept of managing mobile devices (smartphones and tablets) similar to how IT manages computers. Expected features include performance monitoring, encryption, the ability to remotely wipe the device, and so on. BlackBerry Enterprise Server (BES) is the original MDM solution, and now at least a half dozen third-party vendors have entered the space that, in many ways, bring the features IT loves from BES and extends them to Android, iOS, Windows Phone, and webOS.

In the past few years, this space has exploded, but now a newcomer has come to steal the show. It's called mobile application management, or MAM. (Are the acronyms too similar? One thing that helps me is to think of the more casual ma'am vs. the traditional madam.)

Awful puns aside, here's the thesis behind MAM—in today's day and age, many employees are bringing their own smartphones into the Microsoft Exchange Server environment and other corporate networks. (Vendors in the space call it BYOD, or "bring your own device.") In this crazy BYOD world we live in, employees don't want the whole phone managed, monitored, and controlled. And on the same coin, not all employers want to deal with the liability of having that individual's data under their umbrella. (You know, compliance, SOX, all that jazz.) So, MAM comes to the rescue as the best of both worlds, or BOBW. (Sorry, couldn't help adding one more acronym to the mix.)

But does application management alone truly cut it? Let's dive into that question.

What You Get with MAM

I recently spoke with two vendors in the MAM space, AppCentral and Apperian, and while the two are different, there are some commonalities. (I won't dwell on the differences in this article—my purpose is to give you an overview, and you can do your own research and ask all the good questions should you go down that road.)

So here's what you get in a nutshell: You hook up the MAM solution to a client machine, either a software download or a Software as a Service (SaaS) solution. And from here, you can manage both the apps that your company has developed for its employees, and (to some extent) the apps your employees use that came from those big scary app stores.

You can push apps that you develop to your employees and make sure they download them. You can also determine who should get what apps based on department, title, etc.—and those policies can integrate with Active Directory, thankfully. Also, you can recommend specific apps from public app stores to your users, again by department, and you can even restrict users from accessing the public app store beyond what you've recommended if you feel the need to do so. (You can't technically prevent a smartphone user from accessing the iOS or Android stores, but you can set company policies to monitor this and reprimand those who fail to comply.) Oh, and you can also use these solutions to push documents out to mobile devices, such as a PowerPoint slide to the sales team. So there are lots of nifty features there.

Another feature that AppCentral offers (not sure about the rest of the competitors) that's interesting is application purchasing management. This means, you might not want to restrict users from the app store, but you might want to manage how much they're spending (or how much they can spend), and work on bulk licensing so the whole executive team can get Fruit Ninja at a 15 percent discount, or whatever other essential apps you need.

There are plenty of other interesting features, but that should provide a brief overview of what you can expect from an MAM solution.

But What About Device Management?

A valid question to all this is, what about device management? What about performance monitoring, remote wipe, expense management, etc.? Well, most MAM vendors would probably say ActiveSync and BES are sufficient for those needs for most companies. And maybe that's true. But if that's not true for your company, you can also deploy both an MDM and an MAM solution. It's all about choice.

Update from blog: Thanks to @abraunberg on Twitter for pointing out that BoxTone (an MDM vendor) and Apperian are partnering to offer a combined MDM/MAM solution. I don't think they're the only ones doing this (have heard about several MDM vendors that are offering increased application management), but it's interesting to see two well-recognized vendors in these spaces working together.

So in a nutshell, MAM can potentially offer everything you need to manage mobile applications, at a lower cost and lower level of control than MDM solutions. And for many organizations, that's a pretty sweet deal.

—Brian Reinholz

InstantDoc ID 139584

Orchestrator 2012 and Blue Collar / White Collar IT Professionals

In a recent presentation, PowerShell Creator Jeffrey Snover talked about the coming bifurcation of the profession of systems administrator into what he called "Blue Collar" and "White Collar" IT. His argument is that the ongoing trend in the industry is toward fewer people being responsible for more and more servers, and that roles that would likely see wage growth were the ones that drove that consolidation.

Snover prophesied that IT pros who had the ability to heavily automate processes that today required "repetitive click through configuration" were still going to have jobs in the future. Through embracing increasing automation, he said, you will keep yourself relevant and the guys who ignore automation in favor of repetitive configuration will soon find themselves out of a job. Sort of like how you need a whole lot fewer people working on desktop and application deployment when you start to use centralized tools such as System Center Configuration Manager.

Snover predicts that we'll see blue collar, low paid IT jobs and white collar, high paid IT jobs. The blue collar jobs will involve replacing failed hardware on servers—a job that doesn't require a substantial amount of training—and the white collar jobs will focus around admins with the ability to automate complex repetitive processes. Someone will always need to replace the failed hardware, but if your job could be replaced by a complex script it won't be too long until it will be, he predicts.

Snover talked about PowerShell as the golden chalice that systems administrators need to grasp and that admins need to put down their mouse if they want to embrace the future. I think he's partially right in that those that learn to consolidate through automation will still have jobs at the expense of those whose duties can be replaced by complex scripts. What I think he missed is that it isn't just PowerShell that allows you to create powerful automation on the Windows platform. System Center Orchestrator, formerly Opalis, makes it even easier, quicker, and therefore cheaper to automate many complex Windows systems administration tasks.

Although PowerShell is a well designed language that pretty much allows you to do anything on the Windows platform, it still takes time to put together a PowerShell script that can automate a complex task. With Orchestrator's Runbook Designer and product integration packs, putting together a complex set of automated steps for a significant number of tasks becomes a drag-and-drop affair rather than something that needs to be hacked together in a text editor. You can use PowerShell with Orchestrator Runbooks if you find you need to do something that isn't included as an Integration Pack item—but you'll find it a lot simpler to automate processes if you use Orchestrator with PowerShell rather than just using PowerShell by itself.

I think Snover is right in that automation is going to shrink the number of IT professionals needed to manage complex server infrastructure. I disagree with him about admins having to put down the mouse, because with Orchestrator you can use the mouse to automate complex tasks a lot more quickly than you could by bashing out the same automation in PowerShell. Systems administrators who have jobs at the end of the decade will not only believe in the efficiency of automation, but the efficiency in developing that automation.

System Center Orchestrator 2012 is currently in beta and can be downloaded at http://bit.ly/iLBE4e.

—Orin Thomas

InstantDoc ID 139730

Gartner: 77 Percent of CFOs Say IT Service Levels Not Meeting Business Expectations

In a sobering report put together by IT research firm Gartner and the Financial Executives Research Foundation (FERF), a majority of the 344 CFOs interviewed for the study felt that internal IT organizations weren't being managed properly, lacked organizational and technical flexibility, and weren't delivering the technology innovations needed by their respective businesses.

The study revealed that only 35 percent of CFOs viewed their IT departments as being "a strategic driver of business performance", and only 32 percent of respondents saw the CIO "as being a key partner in [business] strategy." Here are more details:

- 30 percent believed their IT organization could deliver against business strategy
- 25 percent believed IT had the right number of skilled people to meet business needs
- 23 percent believed IT service levels met or exceeded business expectations

These findings may not surprise CIOs and senior IT managers, who are increasingly being asked to justify IT expenditures in light of the troubled economy and other pressures on organizations of all sizes. Placed against the backdrop of the larger IT discussion about cloud computing and its potential to reduce IT costs while increasing operational agility—despite concerns about security, compliance, and data preservation in the cloud—the results of this survey should also give IT pros a glimpse into what is on the minds of many CFOs when it comes to IT resources and tech spending these days.

—Jeff James

InstantDoc ID 139703

Self-Inflicted Wounds with Microsoft Outlook

I sent out a Microsoft Office Outlook meeting invite recently for a call I was planning to have—or so I thought. It occurred to me sometime late the night before, as I was wondering why neither of the intended participants had responded, that in fact that was because I hadn't included any invitees on the invite. Big Outlook fail on my part—although I'd like to go ahead and blame Outlook for letting me send an invite with no recipients.

OK, to be technically correct, Outlook didn't send an invite (and obviously, neither did I); because there were no recipients, I merely saved an appointment to my calendar instead of sending a meeting request. What I learned after reviewing my process is that I typically set new meetings by double-clicking the time slot on the calendar, which defaults to an appointment, not a meeting request. You can switch it to a meeting request by clicking Invite Attendees on the Appointment tab of the Ribbon in Outlook 2007. If you don't, your Send button isn't a Send button at all but merely a Save & Close button—which, in practice, looks pretty much the same as if it's sending and closing when you click it.

Obviously, I skipped a crucial step. This morning, when I explained what I'd done to Tony Redmond, one of the intended invitees, he suggested there might be an interesting story in discussing "the worst self-inflicted Outlook wounds." So, here I am. And thanks for the idea and the title, Tony!

This particular mistake certainly is one of the stupider ones I've made. But I'm sure we've all made this sort of glaring Outlook error from time to time—even beyond the unfathomable Reply All on the whole-company distribution list message just to say, "I agree!" I'll spill some of my dirty secrets, and then I hope you'll share with me some of yours.

Sticking on the calendar theme, I've put appointments and reminders on the wrong week, wrong month, and—yes—even wrong year. I've scheduled meetings for times I knew I wasn't going to be at work—but had failed to put such information on my calendar. I've showed up for meetings at the wrong time simply because I failed to actually check my calendar and went with the time that was in my head—not the most reliable storage receptacle.

When it comes to email, sure, I've used Reply All a time or two that I wished I hadn't, but never on a global email list, and never with repercussions. So far. I've also replied to an individual when I intended to Reply All, and then sat wondering why no one was answering the question. I recall one time when I was discussing an article by Paul Robichaux with another editor but in fact I sent my comments to Paul. He responded to me right away to let me know my message had gone astray. Fortunately, I didn't call him any bad names or anything; occasionally, I can maintain a professional demeanor, even if by accident.

Naturally, I've deleted messages that I wished I'd saved. Of course, I've got the Deleted Items folder as a backup, and it's even searchable. Works great—until I forget I'm already in the Deleted Items folder and hit Delete, resulting in the permanent delete. In the piler versus filer debate, I try to be a filer, so I have numerous folders in Outlook designated for saving certain topics. But then I'll drop something in the wrong folder, or forget which folder I decided something belonged in. Search to the rescue again.

More times than I can count, I've intended to send someone an attachment without attaching the attachment; I'm sure just about everyone has made this mistake. I don't think I've ever picked the wrong message recipient from Outlook's Autocomplete, but in a similar vein I have picked the wrong IM recipient from my Office Communicator contacts. Hey, she was the first green-jelly-bean Jill I came to, so I sent her my question. Too bad she had no way of answering it. And what's the big idea of having so many Jills anyway?

I could go on. But I think I won't. Outlook has features set up to prevent some of these problems. For instance, I know there's a warning you get when you try to delete a message from the Deleted Items folder—unless you've chosen to turn off said warning. With Outlook 2010 and Exchange 2010, the MailTips feature can help you avoid some of the message sending embarrassments that are all too common.

Leave a comment at www.windowsitpro.com, InstantDoc ID 139820 with your personal Outlook self-inflicted wounds—or those of your end users.

—B. K. Winstead

InstantDoc ID 139820

DISCOVER WINDOWS IT PRO VIP

Windows IT Pro VIP is the perfect tool for the IT pro who knows that 15 minutes searching the Web is costing more than just time.

WINDOWS IT PRO is:

1. **Educational**—FREE eLearning courses and eBooks to keep your skills sharp
2. **Deep**—over 41,000 articles on DVD and online, some exclusively for VIP members
3. **Broad**—all the articles, solutions, and FAQs ever published in:
   Windows IT Pro
   SQL Server Magazine
   SharePointPro Connections
   DevProConnections
4. **Reliable**—every solution has been road-tested by our experts
5. **Impartial**—with technical editors who are shaping the industry
6. **Economical**—more than $1,000 of resources for less than $17* a month

Upgrade to VIP at windowsitpro.com/go/vip

* Rates vary outside the U.S.

AD INDEX

For detailed information about products in this issue of *Windows IT Pro*, visit the web sites listed below.

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

DIRECTORY OF SERVICES | WINDOWS IT PRO NETWORK

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
www.windowsitpro.com/go/forums

News

Check out the current news and information about Microsoft Windows technologies.
www.windowsitpro.com/go/news

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

DevProConnections UPDATE
Exchange & Outlook UPDATE
Security UPDATE
SharePoint Pro UPDATE
SQL Server Magazine UPDATE
Windows IT Pro UPDATE
WinInfo Daily UPDATE
www.windowsitpro.com/email

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Diane Madzelonka at Diane.madzelonka@penton.com.

Windows IT Pro VIP

Get exclusive access to over 40,000 articles and solutions on CD and via the Web. Includes FREE access to eBooks and archived eLearning events, plus a subscription to either Windows IT Pro or SQL Server Magazine.
www.windowsitpro.com/go/vipsub

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

ASSOCIATED WEBSITES

DevProConnections

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.
www.devproconnections.com

SharePoint Pro

Dive into Microsoft SharePoint content offered in specialized articles, member forums, expert tips, and Web seminars mentored by a community of peers and professionals.
www.sharepointpromag.com

NEW WAYS TO REACH *WINDOWS IT PRO* EDITORS:

LinkedIn: To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

Facebook: We've created a page on Facebook for *Windows IT Pro*, which you can access at: http://tinyurl.com/d5bquf. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

Twitter: Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

Windows IT Pro

Ctrl+Alt+Del

by Jason Bovberg

"Send your funny screenshots, oddball product news, and hilarious end-user stories to rumors @windowsitpro.com. If we use your submission, you'll receive a free gift."

Drink This Column!

PRODUCT OF THE MONTH

Our favorite product this month could just possibly be our favorite product of the year—or the entire existence of this column. That's right, it's a set of Ctrl+Alt+Del coffee mugs immortalizing not only everybody's favorite three keys on the keyboard but also—inadvertently—the page you're reading right now! Available at ThinkGeek, this fabulous set of three mugs are black with a white interior, and each holds eight ounces of your favorite caffeinated beverage. According to the site, just as "hitting those three buttons are designed to interrupt the computers processes, clear out the memory, and recycle system power," these cups will let you "enjoy your personal mental refresh using a coffee-cup set made to look like the keys you use to refresh your computer." The set costs $11.99. Find more information at the ThinkGeek website (www.thinkgeek.com/homeoffice/mugs/e79b/)

USER MOMENT OF THE MONTH

I was working IT for a restaurant chain when this happened. Mind you, I wasn't actually *in* one of the restaurants—just at the head office. Anyway, a user stopped by my desk wondering if everyone was experiencing slow network connectivity. I quickly showed him that access was perfectly smooth and quick on my machine (part of the same network)—Internet and intranet were fine. "Do you mind checking out my system?" he asked. He was just a few doors down, so we went to take a look. I opened Task Manager and found several apps that were frequently using 100 percent of the processor. It didn't take long to realize that the computer was abnormally hot. Leaning over to check the fan, my hand came away smudged with chocolate. Turns out, the whole fan grill was filled with melted chocolate. All the user said was, "Oh."

—Tony

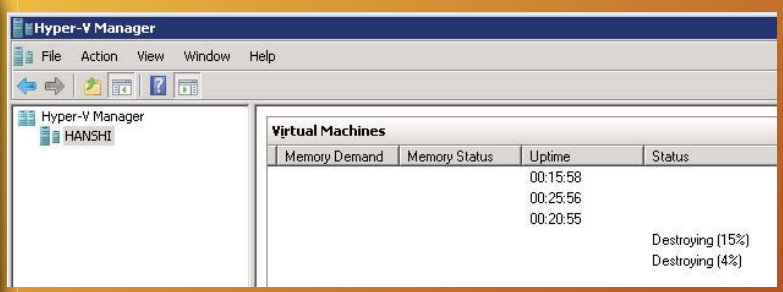


Figure 1: Unsettling terminology

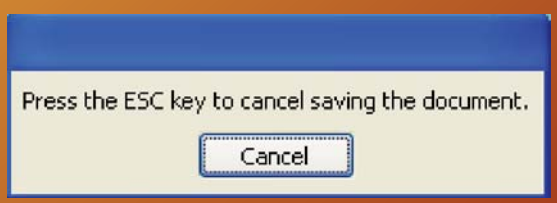
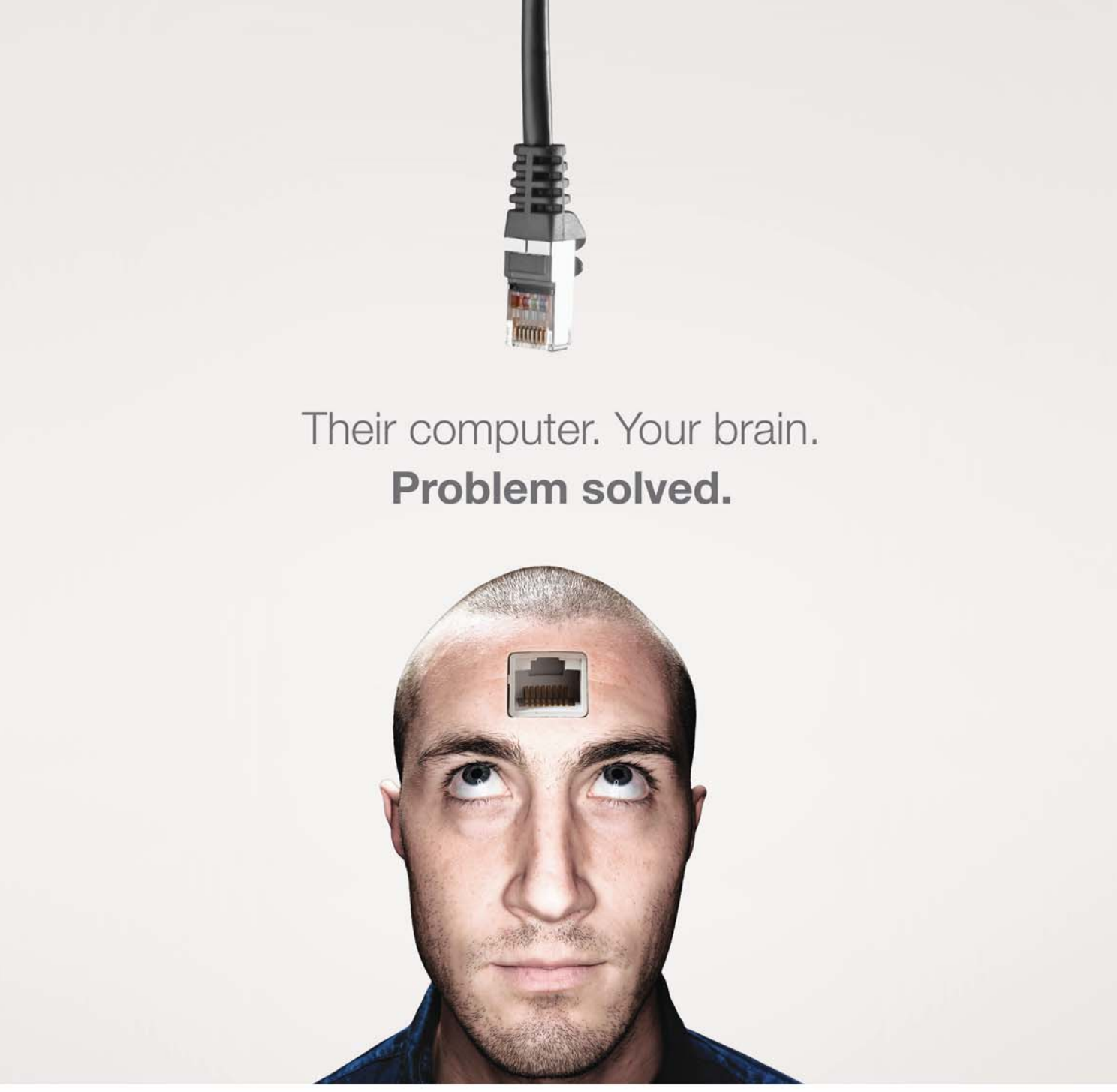


Figure 2: What happens when you click Cancel?

September 2011 issue no. 205, *Windows IT Pro* (ISSN 1552-3136) is published monthly. *Windows IT Pro,* 748 Whalers Way, Fort Collins, CO 80525, (800) 793-5697 or (970) 663-4700. Sales and Marketing Offices: 748 Whalers Way, Fort Collins, CO 80525. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,*** 748 Whalers Way, Fort Collins, CO 80525**. SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, 748 Whalers Way, Fort Collins, CO 80525. Printed in the USA.



Their computer. Your brain.

Problem solved.

Unleash the power of remote support. GoToAssist® is the instant, easy and effective remote support solution that brings your brain and their computer together in problem-solving harmony. Gain immediate remote access and resolve IT issues FAST with GoToAssist, best-of-class live support for your business and customers.

Try it free for 30 days.

1 877 496 9992 | gotoassist.com

GoToAssist

by CITRIX

DB2 on POWER: 3x faster. Check. As low as 1/3 the price. Mate.

Which database has the right moves? DB2® on Power Systems™ performs three times faster per core than Oracle Database on SPARC—based on both TPC-C and SAP® SD benchmarks.* Yet the price of DB2 is as low as 1/3 the price of Oracle Database.** Maybe that's why in 2010 over 1,000 Oracle Database clients chose DB2 instead. Game over.

ibm.com/facts

*PERFORMANCE: www.tpc.org as of 3/28/11 [IBM Power 780 (3 x 64 C)(24 Ch/192 C/768 Th); 10,366,254 tpmC; $1.38/tpmC; avail. 10/13/10 v. Oracle SPARC SuperCluster w/T3–4 Servers (27 x 64 C)(108 Ch/1728 C/13824 Th); 30,249,688 tpmC; $1.01/tpmC; avail. 6/1/11]. TPC-C is a trademark of Transaction Performance Processing Council. 2-tier SAP SD standard application benchmark results as of 3/28/11 [IBM Power 795 (32 P/256 C/1024 Th); 126,063 users, SAP ERP 6.0 EhP4/AIX 7.1 + DB2 9.7; cert. 2010046 v. Oracle SPARC Enterprise Server M9000 (64 P/256 C/512 Th); 39,100 users, SAP ERP 6.0/Solaris 10, Oracle 10g; cert. 2008042] www.sap.com/benchmark. SAP and all SAP logos are trademarks or registered trademarks of SAP AG in Germany and several other countries. **PRICE: based on publicly avail. U.S. info on 2/10/2011 for IBM DB2 Advanced Enterprise Edition + Oracle software w/comparable capabilities. No SAP SD benchmark results are used for any price/performance metrics. IBM: 100 Processor Value Units. Oracle: assumes 1.0 processor multiplier. Both incl. Y1 maint./support. IBM, the IBM logo, ibm.com, DB2, Power Systems, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.